

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2020年9月24日(24.09.2020)



(10) 国際公開番号

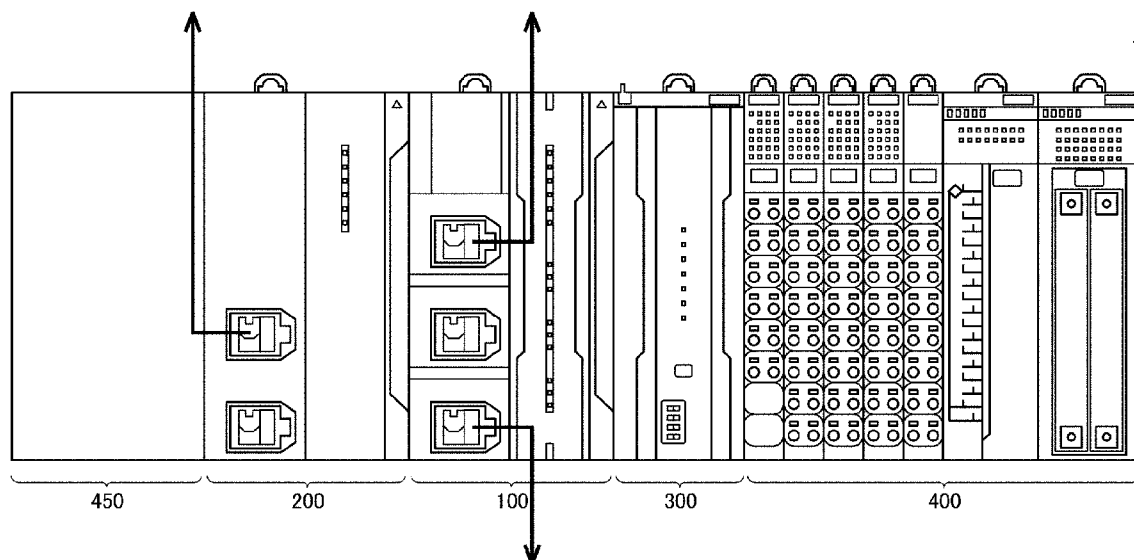
WO 2020/189207 A1

- (51) 国際特許分類:
G05B 19/05 (2006.01) *G05B 9/02* (2006.01)
- (21) 国際出願番号: PCT/JP2020/007802
- (22) 国際出願日: 2020年2月26日(26.02.2020)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2019-047995 2019年3月15日(15.03.2019) JP
- (71) 出願人: オムロン株式会社 (**OMRON CORPORATION**) [JP/JP]; 〒6008530 京都府京都市下京区塩小路通堀川東入南不動堂町801番地 Kyoto (JP).
- (72) 発明者: 永田 雄大(**NAGATA, Yuta**); 〒6008530 京都府京都市下京区塩小路通堀川東入南不動堂町801番地 オムロン株式会社内 Kyoto (JP).
- (74) 代理人: 特許業務法人深見特許事務所(**FUKAMI PATENT OFFICE, P.C.**); 〒5300005 大阪府大阪市北区中之島三丁目2番4号 中之島フェスティバルタワー・ウエスト Osaka (JP).
- (81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,

(54) **Title:** CONTROLLER SYSTEM

(54) 発明の名称: コントローラシステム

FIG.1



(57) **Abstract:** This controller system (1) is provided with: a control unit (100) which executes a control operation for controlling a subject to be controlled; and a security unit (200) which takes charge of a security function for the controller system (1). The security unit (200) includes a detection means for detecting whether there is an incident pertaining to security in the controller system (1). When the incident is detected by the detection means, the control unit (100) transitions a control mode to a degeneration mode and maintains the control mode as the degeneration mode until a release of the incident is detected by the detection means.

ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG,
US, UZ, VC, VN, WS, ZA, ZM, ZW.

- (84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

- 一 国際調査報告 (条約第21条(3))

(57) 要約: コントローラシステム (1) は、制御対象を制御するための制御動作を実行する制御ユニット (100) と、コントローラシステム (1) に対するセキュリティ機能を担当するセキュリティユニット (200) とを備える。セキュリティユニット (200) は、コントローラシステム (1) における、セキュリティに関するインシデントの有無を検知する検知手段を含む。制御ユニット (100) は、検知手段によりインシデントが検知された場合には、制御モードを縮退モードに遷移させて、インシデントの解除が検知手段によって検知されるまで制御モードを縮退モードに保つ。

明 細 書

発明の名称：コントローラシステム

技術分野

[0001] 本発明は、制御対象を制御するコントローラシステムに対するセキュリティ機能に関する。

背景技術

[0002] 各種設備および各設備に配置される各種装置の制御には、ＰＬＣ（プログラマブルロジックコントローラ）などの制御装置が用いられる。制御装置は、制御対象の設備や機械に生じる異常を監視するとともに、制御装置自体の異常を監視することも可能である。何らかの異常が検知されると、制御装置から外部に対して何らかの方法で通知がなされる。

[0003] 例えば、特開２０００－１３７５０６号公報（特許文献１）は、異常履歴が登録されたとき、または、予め定められた時間が到来したときに、予め指定された宛先に電子メールを送信するプログラマブルコントローラを開示する。

先行技術文献

特許文献

[0004] 特許文献１：特開２０００－１３７５０６号公報

発明の概要

発明が解決しようとする課題

[0005] 近年のＩＣＴ（Information and Communication Technology）の進歩に伴って、制御装置も様々な外部装置とネットワーク接続されるとともに、制御装置において実行される処理も高度化している。このようなネットワーク化あるいはインテリジェント化に伴って、想定される脅威の種類も増加している。したがって、このような脅威に対する制御装置および制御システムの保護が必要となっている。制御装置および制御システムに対する脅威が存在する間、その脅威から制御装置および制御システムを保護することの確実性

を高くすることが求められる。

[0006] 本発明は、制御装置および制御システムのネットワーク化あるいはインテリジェント化に伴って生じ得る脅威に対する保護の確実性を高めることを一つの目的としている。

課題を解決するための手段

[0007] 本開示の一例は、コントローラシステムであって、制御対象を制御するための制御動作を実行する制御ユニットと、制御ユニットに接続され、コントローラシステムに対するセキュリティ機能を担当するセキュリティユニットとを備え、制御ユニットは、制御動作に関する制御モードとして、正常モードと、コントローラシステムの限定的な動作を実行するための縮退モードとを有し、正常モードと縮退モードとは相互に遷移可能であり、セキュリティユニットは、コントローラシステムにおける、セキュリティに関するインシデントの有無を検知する検知手段を含み、制御ユニットは、検知手段によりインシデントが検知された場合には、制御モードを縮退モードに遷移させて、インシデントの解除が検知手段によって検知されるまで制御モードを縮退モードに保つ。

[0008] 上記によれば、セキュリティに関するインシデントが解除されるまで、制御ユニットは縮退モードで稼働する。セキュリティに関するインシデントが解除されていないにもかかわらず、制御ユニットが正常モードで稼働することを防止できる。したがって、制御装置および制御システムのネットワーク化あるいはインテリジェント化に伴って生じ得る脅威に対する保護の確実性を高めることができる。

[0009] 好ましくは、制御ユニットは、検知手段からインシデントの検知に関するインシデント情報を取得し、インシデント情報がインシデントの解除を示す場合には、制御ユニットは、縮退モードから正常モードへ制御モードを変更し、インシデント情報がインシデントの継続を示す場合には、制御ユニットは、制御モードを縮退モードに設定する。

[0010] 上記によれば、制御ユニットは、セキュリティユニットからの情報に基づ

いて、制御モードを正常モードまたは縮退モードに設定することができる。
これにより、制御装置および制御システムのネットワーク化あるいはインテリジェント化に伴って生じ得る脅威に対する保護の確実性を高めることができる。

[0011] 好ましくは、制御ユニットは、制御ユニットの再起動処理を実行する場合に、インシデント情報に基づいて、制御モードを決定する。

[0012] 上記によれば、セキュリティに関するインシデントが解除されていない場合には、制御ユニットを再起動した後も制御モードは縮退モードに設定される。インシデントが解除されていないにもかかわらず、制御ユニットの再起動処理によって制御モードが正常モードに設定されることを防止できる。

[0013] 好ましくは、セキュリティユニットは、インシデントの検知に関する情報を不揮発的に記憶して、コントローラシステムへの電源再投入によるコントローラシステムの再起動時に、セキュリティユニットは、セキュリティユニットに記憶された情報に基づいて、セキュリティユニットのステータスを復帰させ、制御ユニットは、セキュリティユニットのステータスに基づいて、制御モードを設定する。

[0014] 上記によれば、セキュリティに関するインシデントが解除されていない場合には、コントローラシステム全体を電源再投入によりリセットしても、セキュリティユニットに記憶された情報に基づいて、制御モードは縮退モードに設定される。インシデントが解除されていないにもかかわらず、コントローラシステムの再起動処理によって制御モードが正常モードに設定されることを防止できる。

[0015] 好ましくは、セキュリティユニットは、管理者権限を持つユーザからの操作をインシデント情報に優先させてインシデントの検知に関するセキュリティユニットのステータスを変更する。

[0016] 上記によれば、たとえばインシデントが解除されたことが明らかな場合に、コントローラシステム 1 を早期に復旧させることができる。

[0017] 好ましくは、縮退モードにおいて、制御ユニットは、制御動作を制限する

。

上記によれば、システムの稼働を維持することができる。

[0018] 好ましくは、縮退モードにおいて、制御ユニットは、制御対象の動作を制限する。

上記によれば、システムの稼働を維持することができる。

発明の効果

[0019] 本発明によれば、制御装置および制御システムのネットワーク化あるいはインテリジェント化に伴って生じ得る脅威に対する保護の確実性を高めることができる。

図面の簡単な説明

[0020] [図1]本実施の形態に係るコントローラシステムの構成例を示す外観図である。

[図2]本実施の形態に従うコントローラシステムを構成する制御ユニットのハードウェア構成例を示す模式図である。

[図3]本実施の形態に従うコントローラシステムを構成するセキュリティユニットのハードウェア構成例を示す模式図である。

[図4]本実施の形態に従うコントローラシステムを構成するセーフティユニットのハードウェア構成例を示す模式図である。

[図5]本実施の形態に従うコントローラシステムを含む制御システムの典型例を示す模式図である。

[図6]セキュリティ脅威に対する対策サイクルの一例を示す模式図である。

[図7]本実施の形態に従うコントローラシステム 1 を含む制御システムにおける不正侵入検知時の対応の一例を示す模式図である。

[図8]生産機械および検査装置を含むラインに対する攻撃例を示す模式図である。

[図9]本実施の形態に従うコントローラシステム 1 におけるインシデント特性に応じた設備別の制御動作の一例を示す図である。

[図10]本実施の形態に従うコントローラシステム 1 におけるインシデント特

性に応じた設備別の制御動作の別の一例を示す図である。

[図11]本実施の形態に従うコントローラシステム1におけるインシデント特性に応じた各設備における状態別の制御動作の一例を示す図である。

[図12]本実施の形態に従うコントローラシステム1におけるセキュリティ脅威が検知された場合の処理手順を示すフローチャートである。

[図13]本実施の形態に従うコントローラシステム1に採用されるインジケータの一例を示す模式図である。

[図14]インシデント発生後の制御システム10の復旧において想定される状態を示した図である。

[図15]図14に示した事態に対応するシステムの状態を示した図である。

[図16]本実施の形態に係る再稼働処理のフローを示すための図である。

[図17]本実施の形態における制御システムの再稼働処理のフローを説明するための第1の図である。

[図18]本実施の形態における制御システムの再稼働処理のフローを説明するための第2の図である。

発明を実施するための形態

[0021] 本発明の実施の形態について、図面を参照しながら詳細に説明する。なお、図中の同一または相当部分については、同一符号を付してその説明は繰り返さない。

[0022] < A. コントローラシステム1 >

まず、本実施の形態に従うコントローラシステム1の構成について説明する。

[0023] 図1は、本実施の形態に係るコントローラシステム1の構成例を示す外観図である。図1を参照して、コントローラシステム1は、制御ユニット100と、セキュリティユニット200と、セーフティユニット300と、1または複数の機能ユニット400と、電源ユニット450とを含む。

[0024] 制御ユニット100とセキュリティユニット200との間は、任意のデータ伝送路（例えば、PCI Express（登録商標）あるいはイーサネ

ット（登録商標）などを介して接続されている。制御ユニット１００とセーフティユニット３００および１または複数の機能ユニット４００との間は、図示しない内部バスを介して接続されている。

[0025] 制御ユニット１００は、コントローラシステム１において中心的な処理を実行する。制御ユニット１００は、任意に設計された要求仕様に従って、制御対象を制御するための制御演算を実行する。後述のセーフティユニット３００で実行される制御演算との対比で、制御ユニット１００で実行される制御演算を「標準制御」とも称す。図１に示す構成例において、制御ユニット１００は、１または複数の通信ポートを有している。

[0026] セキュリティユニット２００は、制御ユニット１００に接続され、コントローラシステム１に対するセキュリティ機能を担当する。図１に示す構成例において、セキュリティユニット２００は、１または複数の通信ポートを有している。セキュリティユニット２００が提供するセキュリティ機能の詳細については、後述する。

[0027] セーフティユニット３００は、制御ユニット１００とは独立して、制御対象に関するセーフティ機能を実現するための制御演算を実行する。セーフティユニット３００で実行される制御演算を「セーフティ制御」とも称す。通常、「セーフティ制御」は、ＩＥＣ ６１５０８などに規定されたセーフティ機能を実現するための要件を満たすように設計される。「セーフティ制御」は、設備や機械などによって人の安全が脅かされることを防止するための処理を総称する。

[0028] 機能ユニット４００は、コントローラシステム１による様々な制御対象に対する制御を実現するための各種機能を提供する。機能ユニット４００は、典型的には、Ｉ／Ｏユニット、セーフティＩ／Ｏユニット、通信ユニット、モーションコントローラユニット、温度調整ユニット、パルスカウンタユニットなどを包含し得る。Ｉ／Ｏユニットとしては、例えば、デジタル入力（ＤＩ）ユニット、デジタル出力（ＤＯ）ユニット、アナログ出力（ＡＩ）ユニット、アナログ出力（ＡＯ）ユニット、パルスキャッチ入力ユニット、お

よび、複数の種類を混合させた複合ユニットなどが挙げられる。セーフティ I/O ユニットは、セーフティ制御に係る I/O 処理を担当する。

[0029] 電源ユニット 450 は、コントローラシステム 1 を構成する各ユニットに対して、所定電圧の電源を供給する。

[0030] < B. 各ユニットのハードウェア構成例 >

次に、本実施の形態に従うコントローラシステム 1 を構成する各ユニットのハードウェア構成例について説明する。

[0031] (b1 : 制御ユニット 100)

図 2 は、本実施の形態に従うコントローラシステム 1 を構成する制御ユニット 100 のハードウェア構成例を示す模式図である。図 2 を参照して、制御ユニット 100 は、主たるコンポーネントとして、CPU (Central Processing Unit) や GPU (Graphical Processing Unit) などのプロセッサ 102 と、チップセット 104 と、主記憶装置 106 と、二次記憶装置 108 と、通信コントローラ 110 と、USB (Universal Serial Bus) コントローラ 112 と、メモリカードインターフェイス 114 と、ネットワークコントローラ 116, 118, 120 と、内部バスコントローラ 122 と、インジケータ 124 とを含む。

[0032] プロセッサ 102 は、二次記憶装置 108 に格納された各種プログラムを読み出して、主記憶装置 106 に展開して実行することで、標準制御に係る制御演算、および、後述するような各種処理を実現する。チップセット 104 は、プロセッサ 102 と各コンポーネントとの間のデータの遣り取りを仲介することで、制御ユニット 100 全体としての処理を実現する。

[0033] 二次記憶装置 108 には、システムプログラムに加えて、システムプログラムが提供する実行環境上で動作する制御プログラムが格納される。

[0034] 通信コントローラ 110 は、セキュリティユニット 200 との間のデータの遣り取りを担当する。通信コントローラ 110 としては、例えば、PCI Express あるいはイーサネットなどに対応する通信チップを採用できる。

- [0035] USBコントローラ112は、USB接続を介して任意の情報処理装置との間のデータの遣り取りを担当する。
- [0036] メモリカードインターフェイス114は、メモリカード115を着脱可能に構成されており、メモリカード115に対して制御プログラムや各種設定などのデータを書込み、あるいは、メモリカード115から制御プログラムや各種設定などのデータを読み出すことが可能になっている。
- [0037] ネットワークコントローラ116, 118, 120の各々は、ネットワークを介した任意のデバイスとの間のデータの遣り取りを担当する。ネットワークコントローラ116, 118, 120は、Ethernet（登録商標）、Ethernet/IP（登録商標）、DeviceNet（登録商標）、Component（登録商標）などの産業用ネットワークプロトコルを採用してもよい。
- [0038] 内部バスコントローラ122は、コントローラシステム1を構成するセーフティユニット300や1または複数の機能ユニット400との間のデータの遣り取りを担当する。内部バスには、メーカ固有の通信プロトコルを用いてもよいし、いずれかの産業用ネットワークプロトコルと同一あるいは準拠した通信プロトコルを用いてもよい。
- [0039] インジケータ124は、制御ユニット100の動作状態などを通知するものであり、ユニット表面に配置された1または複数のLEDなどで構成される。
- [0040] 図2には、プロセッサ102がプログラムを実行することで必要な機能が提供される構成例を示したが、これらの提供される機能の一部または全部を、専用のハードウェア回路（例えば、ASIC（Application Specific Integrated Circuit）またはFPGA（Field-Programmable Gate Array）など）を用いて実装してもよい。あるいは、制御ユニット100の主要部を、汎用的なアーキテクチャに従うハードウェア（例えば、汎用パソコンをベースとした産業用パソコン）を用いて実現してもよい。この場合には、仮想化技術を用いて、用途の異なる複数のOS（Operating System）を並列的に

実行させるとともに、各OS上で必要なアプリケーションを実行させるようにしてもよい。

[0041] (b2:セキュリティユニット200)

図3は、本実施の形態に従うコントローラシステム1を構成するセキュリティユニット200のハードウェア構成例を示す模式図である。図3を参照して、セキュリティユニット200は、主たるコンポーネントとして、CPUやGPUなどのプロセッサ202と、チップセット204と、主記憶装置206と、二次記憶装置208と、通信コントローラ210と、USBコントローラ212と、メモリカードインターフェイス214と、ネットワークコントローラ216, 218と、インジケータ224とを含む。

[0042] プロセッサ202は、二次記憶装置208に格納された各種プログラムを読み出して、主記憶装置206に展開して実行することで、後述するような各種セキュリティ機能を実現する。チップセット204は、プロセッサ202と各コンポーネントとの間のデータの遣り取りを仲介することで、セキュリティユニット200全体としての処理を実現する。

[0043] 二次記憶装置208には、システムプログラムに加えて、システムプログラムが提供する実行環境上で動作するセキュリティシステムプログラムが格納される。

[0044] 通信コントローラ210は、制御ユニット100との間のデータの遣り取りを担当する。通信コントローラ210としては、制御ユニット100に通信コントローラ210と同様に、例えば、PCI Expressあるいはイーサネットなどに対応する通信チップを採用できる。

[0045] USBコントローラ212は、USB接続を介して任意の情報処理装置との間のデータの遣り取りを担当する。

[0046] メモリカードインターフェイス214は、メモリカード215を着脱可能に構成されており、メモリカード215に対して制御プログラムや各種設定などのデータを書込み、あるいは、メモリカード215から制御プログラムや各種設定などのデータを読み出すことが可能になっている。

[0047] ネットワークコントローラ216, 218の各々は、ネットワークを介した任意のデバイスとの間のデータの遣り取りを担当する。ネットワークコントローラ216, 218は、イーサネット（登録商標）などの汎用的なネットワークプロトコルを採用してもよい。

[0048] インジケータ224は、セキュリティユニット200の動作状態などを通知するものであり、ユニット表面に配置された1または複数のLEDなどで構成される。

[0049] 図3には、プロセッサ202がプログラムを実行することで必要な機能が提供される構成例を示したが、これらの提供される機能の一部または全部を、専用のハードウェア回路（例えば、ASICまたはFPGAなど）を用いて実装してもよい。あるいは、セキュリティユニット200の主要部を、汎用的なアーキテクチャに従うハードウェア（例えば、汎用パソコンをベースとした産業用パソコン）を用いて実現してもよい。この場合には、仮想化技術を用いて、用途の異なる複数のOSを並列的に実行させるとともに、各OS上で必要なアプリケーションを実行させるようにしてもよい。

[0050] （b3：セーフティユニット300）

図4は、本実施の形態に従うコントローラシステム1を構成するセーフティユニット300のハードウェア構成例を示す模式図である。図4を参照して、セーフティユニット300は、主たるコンポーネントとして、CPUやGPUなどのプロセッサ302と、チップセット304と、主記憶装置306と、二次記憶装置308と、メモリカードインターフェイス314と、内部バスコントローラ322と、インジケータ324とを含む。

[0051] プロセッサ302は、二次記憶装置308に格納された各種プログラムを読み出して、主記憶装置306に展開して実行することで、セーフティ制御に係る制御演算、および、後述するような各種処理を実現する。チップセット304は、プロセッサ302と各コンポーネントとの間のデータの遣り取りを仲介することで、セーフティユニット300全体としての処理を実現する。

- [0052] 二次記憶装置308には、システムプログラムに加えて、システムプログラムが提供する実行環境上で動作するセーフティプログラムが格納される。
- [0053] メモリカードインターフェイス314は、メモリカード315を着脱可能に構成されており、メモリカード315に対してセーフティプログラムや各種設定などのデータを書込み、あるいは、メモリカード315からセーフティプログラムや各種設定などのデータを読み出すことが可能になっている。
- [0054] 内部バスコントローラ322は、内部バスを介した制御ユニット100との間のデータの遣り取りを担当する。
- [0055] インジケータ324は、セーフティユニット300の動作状態などを通知するものであり、ユニット表面に配置された1または複数のLEDなどで構成される。
- [0056] 図4には、プロセッサ302がプログラムを実行することで必要な機能が提供される構成例を示したが、これらの提供される機能の一部または全部を、専用のハードウェア回路（例えば、ASICまたはFPGAなど）を用いて実装してもよい。あるいは、セーフティユニット300の主要部を、汎用的なアーキテクチャに従うハードウェア（例えば、汎用パソコンをベースとした産業用パソコン）を用いて実現してもよい。この場合には、仮想化技術を用いて、用途の異なる複数のOSを並列的に実行させるとともに、各OS上で必要なアプリケーションを実行させるようにしてもよい。
- [0057] < C. 制御システム10 >
- 次に、本実施の形態に従うコントローラシステム1を含む制御システム10の典型例について説明する。図5は、本実施の形態に従うコントローラシステム1を含む制御システム10の典型例を示す模式図である。
- [0058] 一例として、図5に示す制御システム10は、2つのライン（ラインAおよびラインB）を制御対象とする。典型的には、各ラインは、ワークを搬送するコンベアに加えて、コンベア上のワークに対して任意の物理的作用を与えることが可能なロボットが配置されているとする。
- [0059] ラインAおよびラインBのそれぞれに制御ユニット100が配置されてい

る。ラインAを担当する制御ユニット100に加えて、セキュリティユニット200およびセーフティユニット300がコントローラシステム1を構成する。なお、説明の便宜上、図5には、機能ユニット400および電源ユニット450の記載を省略している。

[0060] コントローラシステム1のセキュリティユニット200は、通信ポート242（図3のネットワークコントローラ216）を介して第1ネットワーク2に接続されている。第1ネットワーク2には、サポート装置600およびSCADA（Supervisory Control And Data Acquisition）装置700が接続されているとする。

[0061] サポート装置600は、少なくとも制御ユニット100にアクセス可能になっており、コントローラシステム1に含まれる各ユニットで実行されるプログラムの作成、デバッグ、各種パラメータの設定などの機能をユーザへ提供する。

[0062] SCADA装置700は、コントローラシステム1での制御演算によって得られる各種情報をオペレータへ提示するとともに、オペレータからの操作に従って、コントローラシステム1に対して内部コマンドなどを生成する。SCADA装置700は、コントローラシステム1が扱うデータを収集する機能も有している。

[0063] コントローラシステム1の制御ユニット100は、通信ポート142（図2のネットワークコントローラ116）を介して第2ネットワーク4に接続されている。第2ネットワーク4には、HMI（Human Machine Interface）800およびデータベース900が接続されているとする。

[0064] HMI800は、コントローラシステム1での制御演算によって得られる各種情報をオペレータへ提示するとともに、オペレータからの操作に従って、コントローラシステム1に対して内部コマンドなどを生成する。データベース900は、コントローラシステム1から送信される各種データ（例えば、各ワークから計測されたトレーサビリティに関する情報など）を収集する。

- [0065] コントローラシステム 1 の制御ユニット 100 は、通信ポート 144（図 2 のネットワークコントローラ 118）を介して、1 または複数のフィールドデバイス 500 と接続されている。フィールドデバイス 500 は、制御対象から制御演算に必要な各種情報を収集するセンサや検出器、および、制御対象に対して何らかの作用を与えるアクチュエータなどを含む。図 5 に示す例では、フィールドデバイス 500 は、ワークに対して何らかの外的な作用を与えるロボット、ワークを搬送するコンベヤ、フィールドに配置されたセンサやアクチュエータとの間で信号を遣り取りする I/O ユニットなどを含む。
- [0066] 同様に、ライン B を担当する制御ユニット 100 についても同様に、通信ポート 144（図 2 のネットワークコントローラ 118）を介して、1 または複数のフィールドデバイス 500 と接続されている。
- [0067] ここで、コントローラシステム 1 の機能面に着目すると、制御ユニット 100 は、標準制御に係る制御演算を実行する処理実行部である制御エンジン 150 と、外部装置との間でデータを遣り取りする情報エンジン 160 とを含む。セキュリティユニット 200 は、後述するようなセキュリティ機能を実現するためのセキュリティエンジン 250 を含む。セーフティユニット 300 は、セーフティ制御に係る制御演算を実行する処理実行部であるセーフティエンジン 350 を含む。
- [0068] 各エンジンは、各ユニットのプロセッサなどの任意のハードウェア要素または各種プログラムなどの任意のソフトウェア要素、あるいは、それら要素の組合せによって実現される。各エンジンは任意の形態で実装できる。
- [0069] さらに、コントローラシステム 1 は、エンジン同士の遣り取りを仲介するブローカー 170 を含む。ブローカー 170 の実体は、制御ユニット 100 およびセキュリティユニット 200 の一方または両方に配置してもよい。
- [0070] 制御エンジン 150 は、制御対象を制御するための制御演算の実行に必要な変数テーブルおよびファンクションブロック（FB）などを保持している。変数テーブルに格納される各変数は、I/O リフレッシュ処理により、フ

フィールドデバイス 500 から取得された値で周期的に収集されるとともに、フィールドデバイス 500 へ各値が周期的に反映される。制御エンジン 150 での制御演算のログはログデータベース 180 に格納されてもよい。

[0071] 情報エンジン 160 は、制御ユニット 100 が保持するデータ（変数テーブルで保持される変数値）に対して任意の情報処理を実行する。典型的には、情報エンジン 160 は、制御ユニット 100 が保持するデータを周期的にデータベース 900 などへ送信する処理を含む。このようなデータの送信には、SQL などが用いられる。

[0072] セキュリティエンジン 250 は、コントローラシステム 1 に発生する不正侵入の検知、検知された不正侵入に応じた処理、インシデントの発生有無判断、発生したインシデントに応じた処理などを実行する。セキュリティエンジン 250 の挙動は、セキュリティ情報 260 として保存される。したがってセキュリティエンジン 250 は、セキュリティに関するインシデントの有無を検知する検知手段に相当する。

[0073] セキュリティエンジン 250 は、セキュリティに関する何らかのイベントが発生したこと、あるいは発生しているセキュリティに関するイベントのレベルなどを、インジケータ 224 で通知する。

[0074] セーフティエンジン 350 は、コントローラシステム 1 において何らかの不正侵入が発生したか否かを検知する検知手段に相当する。セーフティエンジン 350 は、制御ユニット 100 を介して、セーフティ制御に係る制御演算の実行に必要なセーフティ I/O 変数を取得および反映する。セーフティエンジン 350 でのセーフティ制御のログはログデータベース 360 に格納されてもよい。

[0075] ブローカー 170 は、例えば、セキュリティエンジン 250 が何らかのイベントを検知すると、制御エンジン 150、情報エンジン 160 およびセーフティエンジン 350 の動作などを変化させる。

[0076] <D. セキュリティ脅威に対する対策サイクル>

本実施の形態に従うコントローラシステム 1 は、設備や機械を正常運転す

ることを妨げる任意のセキュリティ脅威を検知し、必要な対策を実行可能になっている。

[0077] 本明細書において、「セキュリティ脅威」は、設備や機械を正常運転することを妨げる任意の事象を意味する。ここで、「正常運転」は、システム設計通りおよび生産計画通りに、設備や機械を運転継続できる状態を意味する。なお、システム設計通りおよび生産計画通りに、設備や機械を運転継続するための、設備や機械の立ち上げ、メンテナンス、段取り替えなども付属的な処理も「正常運転」の概念には含まれる。

[0078] PLCを中心とする制御装置においては、典型的には、（１）データベースなどの上位装置からの攻撃、（２）フィールドデバイスからの攻撃、（３）サポート装置を介した攻撃、（４）メモ리카ードなどの制御装置に装着される記憶媒体を介した攻撃、といった４つの局面からのセキュリティ脅威が考えられる。さらに、制御装置に搭載されているすべての物理ポートは攻撃を受けるセキュリティリスクが存在している。

[0079] 本実施の形態に従うセキュリティユニット２００は、これらの各局面で生じるセキュリティ脅威あるいはリスクを検知し、必要な対策が実行できるようにするための処理を実行する。

[0080] 通常、セキュリティ脅威は順次進化するため、セキュリティ脅威に対する対策は継続的に実行する必要がある。このようなセキュリティ脅威に対する継続的な対策について説明する。

[0081] 図６は、セキュリティ脅威に対する対策サイクルの一例を示す模式図である。図６を参照して、セキュリティ脅威に対する対策サイクルは、主として、（１）開発時の対策（ステップＳ１，Ｓ２，Ｓ９）および（２）運用時の対策（ステップＳ３～Ｓ８）に大別される。（１）開発時の対策は、主として、制御対象の設備や機械の設計・仕様を決定する段階における対策を意味し、（２）運用時の対策は、主として、制御対象の設備や機械を運転する段階における対策を意味する。

[0082] より具体的には、まず、制御対象の設備や機械に対する脅威分析が実行さ

れる（ステップS 1）。ステップS 1の脅威分析においては、セキュリティ要件定義が決定される。続いて、セキュリティ機能設計が実行される（ステップS 2）。このセキュリティ機能設計においては、暗号方式、認証方式、アクセス制限などのセキュリティ機能が設計される。

[0083] これらのステップS 1およびS 2において設計された内容が制御対象の設備や機械に反映された上で、運用が開始される。この時点では、通常は正常運転となる（ステップS 3）。上述したように、正常運転は、設備や機械の立ち上げ、本稼働、メンテナンス、段取り替えなどの処理を含む。

[0084] このような正常運転中において、何らかの不正侵入を検知したとすると、セキュリティ脅威1次対応が実行される（ステップS 4）。

[0085] ここで、本明細書において、「不正侵入の検知」あるいは「不正侵入検知」は、何らかのセキュリティ脅威となり得る現象または異常を検知することを意味する。言い換えれば、不正侵入の検知は、通常とは異なる現象または状態の発生を検知することを意味するのみであり、通常インシデントが発生しておらず（但し、インシデントの発生リスク存在している）、また、通常とは異なる現象または状態が不正なものであるか否かを確実に判断することまではできない。そのため、不正侵入が検知されただけでは、すべての処理やイベントをブロックすることは、生産活動を維持する観点からは好ましくない。

[0086] そのため、図6に示されるセキュリティ脅威に対する対策サイクルにおいては、不正侵入が検知されると、1次的な措置として、セキュリティ脅威1次対応が実行される（ステップS 4）。

[0087] セキュリティ脅威1次対応は、インシデント発生リスクがある状況における1次的な措置であり、インシデント発生への進展を防止できる場合もある。仮にインシデントが発生したとしても、セキュリティ脅威1次対応を実行することで、被害を最小限に抑えることができる。本実施の形態に従うコントローラシステム1においては、事前設定することで、セキュリティ脅威1次対応を自動的に実行するようになっている。

[0088] 典型的には、セキュリティ脅威１次対応は、継続、縮退、停止の３つに大別できる。

セキュリティ脅威１次対応の「継続」は、不正侵入が検知される直前と同様に稼働を続行することを意味する。但し、セキュリティ脅威をアラームなどで通知することにより、さらなる対応を迅速に取れる状態としておくのが好ましい。

[0089] セキュリティ脅威１次対応の「縮退」は、コントローラシステムの部分停止（一部のみ稼働）、性能縮小（性能低下）、機能制限などの、限定的ながら稼働を続行することを意味する。すなわち、「縮退」においては、不正侵入が検知される直前の稼働に比較して、ハード面あるいはソフト面で何らかの制限を受けながらも稼働自体は継続する。

[0090] セキュリティ脅威１次対応の「縮退」は、一般的な縮退運転（フォールバック）も含み得る。このような一般的な縮退運転は、システムの機能や性能を部分的に停止させた状態で稼働を維持することを意味する。縮退運転に切り替えた後には、利用できる機能が最低限に抑制され、あるいは、応答速度が低下するといった状態になることが多い。したがって「縮退」は、制御ユニット１００の制御動作を制限すること、制御対象の動作を制限すること、のいずれであってもよい。

[0091] セキュリティ脅威１次対応の「停止」は、安全にシステムの動作を止めることを意味する。

[0092] このようなセキュリティ脅威１次対応が実行された後に、復旧作業が実行される。図５に示すような制御システム１０においては、コントローラシステム１およびコントローラシステム１のフィールド側は、ＯＴ（Operation Technology）部門の作業者が担当し、コントローラシステム１の上位側（第１ネットワーク２および第２ネットワーク４ならびに各ネットワークに接続される装置）については、ＩＴ（Information Technology）部門の作業者が担当する。

[0093] より具体的には、ＯＴ部門の作業者は、制御対象の設備や機械に対して必

要な処理を行う（現場対応）（ステップS 5）。具体的には、設備や機械の復旧作業や監視などの作業が実行される。一方、IT部門の作業者は、発生したセキュリティ脅威に対する脅威解析およびその対策などを行う（ステップS 6）。IT部門の作業者による対策は、暫定的なものと、恒久的なものとを含み得る場合もある。

[0094] OT部門およびIT部門の作業者による対策が完了すると、試運転が実行される（ステップS 7）。この試運転が問題なければ、運用が再開され、正常運転に復帰する（ステップS 3）。

[0095] 一方、セキュリティ脅威1次対応を実行したものの（ステップS 4）、インシデントが発生すると、インシデント対応が実行される（ステップS 8）。インシデント対応は、インシデントが発生した後の対応であり、現場復旧や影響範囲を限定するために緊急的に行う措置を含む。本実施の形態に従うコントローラシステム1においては、事前設定することで、インシデント対応についても自動的に実行するようになっている。

[0096] インシデント対応が実行された後に、OT部門の作業者は、制御対象の設備や機械に対して必要な処理を行う（現場対応）（ステップS 5）とともに、IT部門の作業者は、発生したセキュリティ脅威に対する脅威解析およびその対策などを行う（ステップS 6）。さらに、インシデントレポートが作成され（ステップS 9）、その作成されたインシデントレポートの内容に基づいて、脅威分析（ステップS 1）およびセキュリティ機能設計（ステップS 2）などが再度実行される。

[0097] このように、インシデントが発生した場合には、その発生したインシデントの内容が開発段階までフィードバックされることになる。

[0098] なお、インシデントレポートは、インシデントが発生していなくても作成するようにしてもよい。

[0099] 後述するように、本実施の形態に従うコントローラシステム1は、図6に示すセキュリティ脅威に対する対策サイクルを確実に実行できるような仕組みを提供する。

[0100] < E. セキュリティ脅威 1 次対応 >

次に、図 6 に示されるセキュリティ脅威 1 次対応（ステップ S 4）について説明する。

[0101] （ e 1 : 制御システム 1 0 でのセキュリティ脅威 1 次対応）

まず、制御システム 1 0 に生じる不正侵入（セキュリティ脅威）の検知およびそれに応じたセキュリティ脅威 1 次対応の一例について説明する。

[0102] 図 7 は、本実施の形態に従うコントローラシステム 1 を含む制御システム 1 0 における不正侵入検知時の対応の一例を示す模式図である。図 7 には、図 5 に示す制御システム 1 0 において、SCADA 装置 7 0 0 がウィルスに感染して、第 1 ネットワーク 2 およびセキュリティユニット 2 0 0 の通信ポート 2 4 2 から攻撃された例を示す。

[0103] 図 7 に示す例では、ライン A を担当するコントローラシステム 1 に対してのみ攻撃されており、ライン B を担当する制御ユニット 1 0 0 に対する攻撃はないものとする。セキュリティユニット 2 0 0 は、不正侵入を検知すると、その検知した不正侵入のインシデント特性を制御ユニット 1 0 0 などへ通知する。

[0104] 本明細書において、「インシデント特性」は、検知された不正侵入（セキュリティ脅威）の属性（例えば、攻撃種類、攻撃特性、攻撃レベル、深刻度、緊急度など）を包含する用語である。セキュリティユニット 2 0 0 のセキュリティエンジン 2 5 0 は、予め定められた検知ロジックに基づいて、検知した不正侵入（セキュリティ脅威）のインシデント特性を決定し、制御ユニット 1 0 0 などへ出力する。すなわち、セキュリティユニット 2 0 0 のセキュリティエンジン 2 5 0 は、検知機能により検知された不正侵入の属性を示すインシデント特性を制御ユニット 1 0 0 へ通知する通知手段として機能する。

[0105] 制御ユニット 1 0 0 は、セキュリティユニット 2 0 0 からのインシデント特性に応じた、セキュリティ脅威 1 次対応および／またはインシデント対応を実行する。すなわち、制御ユニット 1 0 0 は、セキュリティユニット 2 0

0のセキュリティエンジン250から通知されたインシデント特性に応じて、制御動作を変更する。

[0106] 図7には、セキュリティ脅威1次対応が実行される例を示す。具体的には、コンベア上を搬送されるワークをロボットで加工するようなラインAを想定する。このようなラインAにおいて、不正侵入が検知されることで、一例として、ワークを加工するロボットを安全に停止させるとともに、コンベア上の仕掛品のワークを倉庫へ退避する処理がセキュリティ脅威1次対応として実行される。

[0107] このようなセキュリティ脅威1次対応を実現するにあたって、制御ユニット100の制御エンジン150は、ラインAについて、ロボットを安全に停止するとともに、コンベア上の仕掛品を倉庫に移動する処理を実行する（ステップS41）。制御エンジン150が出力する命令に従って、フィールドデバイス500のロボットは安全停止（停止）し（ステップS42）、フィールドデバイス500のコンベアは搬送のスピードを低速に切り替えるとともに、仕掛品を倉庫へ移動させるための特殊仕分け処理を実行（縮退）する（ステップS43）。一方、フィールドデバイス500のI/Oユニットは、運転（動作）を継続する（ステップS44）。I/Oユニットが周期的に更新する入出力データは、制御エンジン150が適切に処理を実行するために必要になるからである。

[0108] また、上述したように、図7に示すSCADA装置700からの攻撃では、ラインBを担当する制御ユニット100には影響はないので、ラインBを担当する制御ユニット100の制御エンジン150は運転を継続する（ステップS45）。

[0109] また、制御ユニット100の通信ポート142については、生産継続のための最小限の通信のみを許可するようにしてもよい（ステップS46）。すなわち、制御ユニット100の通信物理ポートの通信を制御するようにしてもよい。なお、制御ユニット100の通信物理ポートに限らず、何らかの不正侵入（セキュリティ脅威）が検知されると、セキュリティユニット200

および／またはセーフティユニット３００の任意の通信物理ポートの通信を制限するようにしてもよい。

[0110] また、制御ユニット１００は、不正侵入（セキュリティ脅威）が検知を知らせるアラームをＨＭＩ８００のインジケータ８２４に表示する（ステップＳ４７）。

[0111] さらに、制御ユニット１００は、セキュリティユニット２００からインシデントの発生を受けると、インシデントレポートをＨＭＩ８００に表示してもよい（ステップＳ４８）。

[0112] 図７に示すように、コントローラシステム１は、不正侵入（セキュリティ脅威）を検知すると、当該検知された不正侵入のインシデント特性に応じたセキュリティ脅威１次対応を実行できる。

[0113] （e２：その他の設備／機械でのセキュリティ脅威１次対応）

上述の図７においては、コンベア上のワークに対して任意の物理的作用を与えることが可能なロボットが配置されたラインを制御対象とする制御システム１０において、ＳＣＡＤＡ装置から攻撃を受けた場合のセキュリティ脅威１次対応について例示した。しかしながら、セキュリティ脅威１次対応は、少なくとも、制御対象に含まれる設備や機械、および、インシデント特性に応じて、対応内容を異ならせることが好ましい。

[0114] （i）加工機に対するデータ改ざんの攻撃

例えば、ＮＣ（Numerical Control）などによるワークの加工機に対して、加工データ（仕上がり形状などを規定したデータ）が改ざんされたような場合を想定する。この場合、加工機および加工機の周辺設備の制御に関しては、セキュリティ脅威１次対応として停止が採用され、人の安全が優先されることになる。

[0115] 一方、情報通信処理に関しては、基本的には、通信を遮断して他の設備から隔離する（情報通信処理）とともに、データ改ざんの攻撃を受けた後に加工されたワークを特定する（情報処理）といったセキュリティ脅威１次対応が採用される。

[0116] (i i) 充填機に対するDDoS攻撃

例えば、缶や瓶などへの液体の充填機（ボトリングマシーン）に対するDDoS（Distributed Denial of Service）攻撃を想定する。通常、充填機は高速に充填動作を行っているので、急停止させることは、設備に対するダメージおよび充填中の缶または瓶の後処理といった面で問題が生じ得る。一方で、DDoS攻撃は、外部との通信が影響を受けるだけであり、充填機自体を動作させることは可能である場合が多い。そのため、充填機は正常運転または縮退運転（例えば、搬送速度を緩やかに低下させる）といったセキュリティ脅威1次対応がとられる。

[0117] 一方、制御ユニット100における情報通信処理に関しては、基本的には、通信を遮断して他の設備から隔離する（通信処理）とともに、データ改ざんの攻撃を受けた後に加工されたワークを特定する（情報処理）といったセキュリティ脅威1次対応が採用される。

[0118] 一方、情報通信処理に関しては、情報を受信する処理（すなわち、DDoS攻撃の対象）については遮断し、情報を送信する処理（例えば、上位サーバへの生産情報の送信）については有効化を継続する。

[0119] このように、制御対象に含まれる設備や機械、および、インシデント特性に応じて、対応内容を異ならせることが好ましい。

[0120] <F. インシデントに応じた対応>

次に、図6に示されるインシデント対応（ステップS8）について説明する。

[0121] 図8は、生産機械および検査装置を含むラインに対する攻撃例を示す模式図である。図8を参照して、例えば、生産機械が製品を生産するとともに、生産機械の下流側に配置された検査装置によって生産機械が生産した製品を検査した上で出荷するようなラインを想定する。

[0122] このようなラインに対して、攻撃者は、不良品を市場に流出させることを目論んだとする。このような目論みを実現するために、攻撃者は、不良品を生産するように生産機械を改ざんし、さらに、その不良品を検出できないよ

うに検査装置を改ざんする。

[0123] このような攻撃の具体的な内容としては、例えば、検査装置に対して、良否判定ロジックを改ざんする。すなわち、検査装置が不良品であると判断しないように、良否判定ロジックを意図的に書き換えるといった攻撃がなされる。

[0124] 併せて、生産機械に対して、レシピ情報および／または制御ロジックを改ざんする。すなわち、生産機械が不良品を生産するように制御内容を変更するといった攻撃がなされる。

[0125] このような攻撃を受けた場合には、インシデントの発生となり、インシデントに応じた対応が必要となる。インシデントに応じた対応についても、インシデント特性に応じてその対応内容を変化させることが好ましい。

[0126] 本事例において、具体的なインシデントに応じた対応としては、以下のようものが想定される。

[0127] ・改ざんされた可能性のある検査装置を使用せずに、別の検査装置に切り替える（検査装置を冗長化しておく、あるいは、別のラインにある安全な検査装置へ製品を流す）

・改ざん前のロジック（良否判定ロジックあるいは制御ロジック）をバックアップしておき、自動的にリストアする（自動的にリストアすることで、エンドユーザが定期的にバックアップをとらなくてもよく、また、安全と判断できる過去のバックアップがどれなのかを特定できる）

・リスクが存在し得る工程の生産を停止する一方で、その他の脅威がない工程については生産を継続する（仕掛品が増加するが、全工程を止める必要はない）

・既に生産された製品の良否判定結果も疑わしいので、正規の倉庫へ保管するのではなく、再度検査を行うことで、そのまま市場へ流通させない（再検査用のラインへ流すようにしてもよいし、人手で再検査してもよい）

上述したように本実施の形態においては、検知された不正侵入（セキュリティ脅威）のインシデント特性を利用できるので、例えば、製品の良否判定

が適切に実行されていることが保証できれば、生産ラインを全停止する必要はない。また、再検査の対象となる商品を絞り込むことができれば、全品回収などの被害拡大を回避できる。

[0128] <G. インシデント特性に応じた対応>

上述したように、本実施の形態に従うコントローラシステム1においては、セキュリティユニット200が不正侵入（セキュリティ脅威）を検知すると、その検知された不正侵入（セキュリティ脅威）のインシデント特性を制御ユニット100などに通知する（図7など参照）。制御ユニット100およびセーフティユニット300においては、インシデント特性に基づいて、セキュリティ脅威に対する適切な範囲および内容の対応が可能となる（図6のステップS4およびS8）。

[0129] 本実施の形態に従うコントローラシステム1は、検知された不正侵入（セキュリティ脅威）のインシデント特性に応じて、制御ユニット100および／またはセーフティユニット300における制御（すなわち、セキュリティ脅威1次対応またはインシデント対応）の内容を異ならせることができる。以下、このようなインシデント特性に応じた制御内容の決定例について説明する。

[0130] 図9は、本実施の形態に従うコントローラシステム1におけるインシデント特性に応じた設備別の制御動作の一例を示す図である。図10は、本実施の形態に従うコントローラシステム1におけるインシデント特性に応じた設備別の制御動作の別の一例を示す図である。図11は、本実施の形態に従うコントローラシステム1におけるインシデント特性に応じた各設備における状態別の制御動作の一例を示す図である。

[0131] 図9には、インシデント特性として、攻撃の種類あるいは攻撃後の状態（例えば、無作為改ざん、リソース枯渇、DDoS攻撃など）がセキュリティユニット200から出力される例を示す。セキュリティユニット200から出力される各インシデント特性に応じた対応が実行されることになる。このようなインシデント特性に応じた対応は、設備や機械毎にさらに細かく設定

されてもよい。

[0132] インシデント特性に応じた対応としては、設備制御についての対応、および、情報通信についての対応に大別できる。設備制御は、主として、制御ユニット100の制御エンジン150および／またはセーフティユニット300のセーフティエンジン350（いずれも図5参照）が担当する処理を意味し、制御対象の設備や機械の動作についての対応を意味する。情報通信は、主として、制御ユニット100の情報エンジン160が担当する処理を意味し、制御ユニット100と外部装置との間のデータの遣り取りや、制御ユニット100内部での情報の取り扱いなどについての対応を意味する。

[0133] 図9に示す制御動作のうち、「正常運転」は、システム設計通りおよび生産計画通りに、設備や機械を運転継続できる状態を意味する。「縮退」（図中には、「縮退」に「A1」などの識別情報を付加して表現している。）は、コントローラシステム1の部分停止（一部のみ稼働）、性能縮小（性能低下）、機能制限などの、限定的ながら稼働を続行することを意味する。「停止」は、安全に、対象の設備や機械あるいはコントローラシステム1の動作を止めることを意味する。なお、図10および図11においても同様である。

[0134] 図10には、インシデント特性としては、検知された不正侵入（セキュリティ脅威）のレベル（重篤度あるいは緊急度など）がセキュリティユニット200から出力される例を示す。各レベルは、検知された攻撃の種類あるいは攻撃後の状態などに基づいて算出される。セキュリティユニット200から出力される各インシデント特性に応じた対応が実行されることになる。このようなインシデント特性に応じた対応は、設備や機械毎にさらに細かく設定されてもよい。

[0135] 図11には、各設備や機械の状態毎に各インシデント特性に応じた対応を設定する例を示す。例えば、設備毎に運転中、メンテナンス中、段取り替え中などの状態を特定するとともに、検知されたインシデント特性と、現在の状態とに基づいて、各設備に対する対応を決定してもよい。

[0136] なお、図 11 には、設備や機械の状態を例示するが、これに限らず、例えば、PLC の動作状態（通常運転中、リモートアクセス中、デバッグ中など）に応じて、対応の内容を異ならせてもよい。さらに、各インシデント特性に応じた対応を状態のみに基づいて決定してもよい。すなわち、設備や機械の違いによらず、セキュリティ脅威が検知されたときの状態のみに基づいて対応を決定するようにしてもよい。

[0137] また、図 11 に示すインシデント特性として、図 10 に示すレベルを用いてもよい。

図 9～図 11 に示すように、本実施の形態に従うコントローラシステム 1 においては、セキュリティユニット 200 から出力されるインシデント特性に応じて、設備毎および／または状態毎に必要な対応を動的に決定できる。このような対応の内容を動的に決定することで、設備や機械の運転を継続することによる生産性の維持と、セキュリティに対する対処とを柔軟に実行できる。なお、図 9～図 11 には、標準制御に関する制御動作を例示するが、セーフティ制御についても同様の制御動作を定義できる。

[0138] 次に、図 9～図 11 に示す「縮退」の一例について説明する。

（１）設備制御の縮退

設備制御の縮退は、範囲、機能、生産性などの面において制限を受けた状態で運転することを意味する。

[0139] 範囲としては、制御対象となるゾーンを制限することができる。制御対象となるゾーンとしては、例えば、制御装置、制御装置に装着されるモジュール、制御装置に装着されるユニットなどの制御側を制限することができる。あるいは、特定の機械、ライン、フロア、工場全体といった被制御側（制御対象）を制限することができる。

[0140] 機能としては、コントローラシステム 1 が提供する処理のうち特定の処理（例えば、情報制御、標準制御、セーフティ制御など）を制限することができる。

[0141] 生産性としては、安全、安心のために一時的に生産性（例えば、ラインス

ピード、単位時間あたりの生産数、単位時間あたりの生産量など）を制限することができる。

[0142] (2) 情報通信の縮退

情報通信の縮退は、範囲、方向、帯域、QoS (Quality of Service)、データなどの面において制限を受けた状態で運転することを意味する。

[0143] 範囲としては、例えば、通信物理ポート、通信論理ポート、ネットワーク離脱などを制限できる。

[0144] 通信物理ポートを制限する場合には、制御ユニット100およびセキュリティユニット200にそれぞれ配置されている通信ポートのうち特定のポート使用を制限することができる。あるいは、コントローラシステム1に実装される通信ポートのうち、上位側あるいはフィールド側のみを有効化してもよい。

[0145] 通信論理ポートを制限する場合には、利用可能なTCP/UDPポートを制限してもよいし、利用可能な通信プロトコルを制限してもよい。さらに、アクセスを受け付けるMACアドレスやIPアドレスを制限してもよい。

[0146] 方向としては、例えば、各ポートにおいてデータが流れる方向を一方向のみに制限してもよい。例えば、特定のポートについて、データの受信のみ許可、あるいは、データの送信のみ許可といった具合である。このような一方向のデータのみを許可することで、何らかのセキュリティ脅威が検知されたときに、コントローラシステム1からデータが流出することを防止できる。

[0147] 帯域としては、コントローラシステム1の通信負荷あるいは処理負荷を低減させるために、通信速度を制限（例えば、1Gbpsから100Mbpsに変更）してもよい。

[0148] QoSとしては、通過させるパケットの優先度を動的に変化させてもよい。例えば、何らかのセキュリティ脅威が検知された場合には、通過させるパケットの優先度を高く変更してもよい。

[0149] データとしては、例えば、Ethernetなどの産業用ネットワークプロトコルにおいては、プロセスデータ通信の有効/無効の切り替えや、出力

値の更新を制限（更新停止／ゼロクリア／前回値を保持など）してもよい。

[0150] 上述したものに限らず、「縮退」は、正常運転に対して任意の制限が加えられた状態での運転を包含し得る。なお、「縮退」は、部分停止と見なすこともでき、「停止」は、特定の機能を全面的に停止することを包含し得るので、「縮退」を拡張した概念と見なすこともできる。

[0151] 図12は、本実施の形態に従うコントローラシステム1におけるセキュリティ脅威が検知された場合の処理手順を示すフローチャートである。図12に示す各ステップは、制御ユニット100のプロセッサ102、セキュリティユニット200のプロセッサ202、およびセーフティユニット300のプロセッサ302がそれぞれプログラムを実行することで実現される。

[0152] 図12を参照して、セキュリティユニット200は、制御ユニット100で生じる処理、および、ネットワーク上を流れるパケットなどに基づいて、不正侵入が生じているか否かを判断する（ステップS100）。不正侵入が生じていなければ（ステップS100においてNO）、ステップS100の処理が繰り返される。

[0153] 不正侵入が生じていなければ（ステップS100においてYES）、セキュリティユニット200は、検知した不正侵入（セキュリティ脅威）に対応するインシデント特性を制御ユニット100へ通知する（ステップS102）。制御ユニット100は、セキュリティユニット200からのインシデント特性の通知を受けて、予め定められた動作の変更に係る条件に合致するか否かを判断する（ステップS104）。

[0154] 予め定められた動作の変更に係る条件に合致すれば（ステップS104においてYES）、制御ユニット100は、当該合致した条件に対応する対象の設備や機械の動作を変更する（ステップS106）。

[0155] これに対して、予め定められた動作の変更に係る条件に合致しなければ（ステップS104においてNO）、ステップS106の処理はスキップされる。そして、ステップS100以下の処理が繰り返される。

[0156] <H. セキュリティ情報の可視化・ユーザ支援>

通常、セキュリティ事象は目に見えないので、特に、OT部門の作業者にとってみれば、現在どのようなステータスであるのかを把握することが難しい。そのため、本実施の形態に従うコントローラシステム1は、セキュリティ情報を可視化するとともに、不正侵入が検知されたときなどのユーザ支援を提供する。

[0157] (h1:ステータス)

セキュリティユニット200が何らかの不正侵入を検知した場合には、セキュリティユニット200の表面に配置されたインジケータ224、制御ユニット100の表面に配置されたインジケータ124、HMI800のインジケータ824（いずれも図5参照）などを用いて、ユーザに通知を行うようにしてもよい。この場合、不正侵入の検知前後で、点灯色変更、点灯開始、点滅開始などの任意の表示態様の変化を利用すればよい。さらに、表示だけではなく、音や音声メッセージなどを用いてもよい。

[0158] セキュリティ脅威は、セキュリティリスクに応じて定量化することもできる。本明細書において、「セキュリティリスク」は、不正侵入として検知される確率あるいは度合いを定量的に示す用語である。「セキュリティリスク」は、例えば、無作為改ざんを行うためのパケットの到来頻度やDDoS攻撃の度合いなどにより算出できる。このような定量化されたセキュリティリスクが得られる場合には、制御ユニット100の表面に配置されたインジケータ124、HMI800のインジケータ824には、算出される度合いを表示するようにしてもよい。

[0159] 図13は、本実施の形態に従うコントローラシステム1に採用されるインジケータの一例を示す模式図である。図13には、定量化されたセキュリティリスクを表示する場合の構成例を示す。たとえばインジケータ224において、3つのLEDが配置されている。3つのLEDの点灯色は、それぞれ緑色、黄色、赤色である。リスクレベルが低いときには緑色LEDのみが点灯する。リスクレベルが中であるときには、緑色LEDおよび黄色LEDが点灯する。リスクレベルが高であるときには、緑色LED、黄色LEDおよ

び、赤色ＬＥＤが点灯する。

[0160] このように、セキュリティユニット２００は、検知手段であるセキュリティエンジン２５０による検知動作から算出されるセキュリティリスクをユーザに提示する提示手段を有している。上述したようなインジケータ２２４を配置することで、専門知識のない作業員であっても、現在のセキュリティリスクのステータスを容易に把握できる。なお、図１３に示すようなインジケータに限らず、セキュリティリスクを提示できる形態であれば、どのようなインジケータを採用してもよい。

[0161] ＜Ⅰ．システムの復旧時における課題＞

セキュリティリスクが発生する確率は小さいほど好ましい。しかしその一方で、ユーザにとっては、セキュリティリスクが発生したときに適切な処理を行う機会が少なくなる。このために、インジケータ２２４によって示される事象（セキュリティリスクの発生）を作業員が正確に把握できない可能性も生じうる。たとえばユーザが、黄色ＬＥＤの点灯を、コントローラシステム１の動作の異常（たとえばプログラムの暴走）と判断することも想定される。このような場合には、ユーザがシステムを誤って再起動（リセット）する可能性がある。

[0162] 図１４は、インシデント発生後の制御システム１０の復旧において想定される事態を示した図である。制御システム１０の動作時に、セキュリティインシデントが発生する。あるいはセキュリティユニット２００においてセキュリティリスクが検知される（ステップＳ１０１）。

[0163] この場合、ＦＡ（Factory Automation）装置／制御システム１０が縮退動作を行う、あるいは一時的に停止する（ステップＳ１０２）。ＩＴ部門のエンジニアは、セキュリティインシデントの解消のために復旧および対策作業を実行する（ステップＳ１０３）。

[0164] 一方、ＯＴ部門のエンジニアは、制御システム１０（生産システム）を再稼働する。しかし、インシデントが解消されていない状態では、制御システム１０が誤って再稼働されることになる（ステップＳ１０４）。この場合、

セキュリティ被害が拡大し、たとえば情報の漏洩、装置の故障等が生じる可能性がある（ステップS105）。

[0165] あるいは、制御システム10が再稼働した後に、再びセキュリティインシデント（またはセキュリティリスク）が検知される（ステップS106）。この場合、FA装置／制御システム10が再び縮退または一時的に停止する（ステップS102）。このように、ステップS102～S106の処理が何度も繰り返される可能性がある。

[0166] 図15は、図14に示した事態に対応するシステムの状態を示した図である。図15を参照して、制御ユニット100（図15では「PLC」と表記）は、制御モードとして、「Run」モードおよび「Safe」モードを有する。Runモードは正常モードである。Safeモードは縮退モードであり、コントローラシステム1の限定的な動作を実行するためのモードである。

[0167] セキュリティユニット200のセキュリティエンジン250は、セキュリティリスクに応じたセキュリティレベル（Lv）として、「Green」、「Yellow」、「Red」の3つのレベルを検知する。「Green」、「Yellow」、「Red」は、インジケータ224のLEDの点灯色にも対応する。Greenレベルはセキュリティが安全なときのレベルである。Yellowレベルは、インシデントが検知されたときのレベルである。Redレベルはインシデントが発生したときのレベルである。

[0168] コントローラシステムの正常稼働時には、制御モードはRunモードであり、セキュリティレベルはGreenレベルである。インシデントが検知されると、セキュリティレベルが「Green」から「Yellow」へと変化するとともに、制御モードがRunモードからSafeモードに遷移する。

[0169] この状態で、制御ユニット100を復旧させたとする。制御モードはSafeモードからRunモードへと復帰する。しかし、セキュリティユニット200で検知されるセキュリティレベルは「Red」である。すなわちイン

シデントは解除されていない。インシデントが解除されないまま制御ユニット100に通常の動作を行わせることによって、セキュリティ被害が拡大する可能性がある。

[0170] あるいは、制御ユニット100を一旦復旧させることにより、制御モードをRunモードに戻しても、インシデントが解除されていないため、制御モードがSafeモードへと移行する。インシデントが解除されない間は、制御ユニット100を復旧させてもインシデントの検知によって、制御モードは一旦Runモードに戻るものの、Safeモードへと移行する。インシデントが解除されていないにもかかわらず、制御ユニット100の復旧を繰り返すことにより、制御モードの遷移に無限ループが生じることも起こり得る。

[0171] <J. インシデント解除のチェック>

本実施の形態では、制御ユニットの再稼働処理のフローの中に、インシデント解除のチェックロジックが含まれる。これによりコントローラシステムの誤った再稼働を防止できるので、セキュリティ被害（2次被害）の拡大を防ぐことができる。

[0172] 図16は、本実施の形態に係る再稼働処理のフローを示すための図である。インシデントを検知したときに、制御ユニット100の制御モードはRunモードからSafeモードに遷移する。この点については既に説明したのでここでは説明を繰り返さない。本実施の形態では、インシデントが解除されるまで、制御モードはRunモードに遷移することができない。したがって制御モードはSafeモードのままに保たれる。

[0173] インシデントが解除された後、セキュリティレベルは「Green」レベルになる。この状態で制御ユニット100のみを復旧させる。たとえば制御ユニット100は再起動処理を実行する。制御モードがSafeモードからRunモードへと遷移して、制御システムが正常に稼働する。セキュリティレベルがGreen以外のレベル（YellowまたはRed）である状態で、制御ユニット100を再起動（リセット）しても、制御ユニット100

の制御モードはS a f eモードである。

[0174] 本実施の形態では、制御モードをS a f eモードからR u nモードへと復帰させる際に、セキュリティレベルがチェックされる。セキュリティレベルがG r e e nであれば、制御モードをS a f eモードからR u nモードに復帰することができる。逆に、インシデントの検知によって、セキュリティレベルがG r e e n以外のレベル（Y e l l o wまたはR e d）である場合、制御モードはS a f eモードに保たれる。

[0175] コントローラシステム1の再起動のために、コントローラシステム1の全体の電源を一旦切って、その後にコントローラシステム1に電源を再投入することも考えられる。しかしセキュリティユニット200は、ステータスあるいはセキュリティレベルに関する情報を不揮発的に保持する。したがって、コントローラシステム1に電源を再投入した場合、セキュリティユニット200に記憶された情報に基づいて、セキュリティユニット200は、セキュリティレベルを設定する。これにより、コントローラシステム1の電源切断前のセキュリティユニット200のステータスが保持される。ステータスあるいはセキュリティレベルに関する情報は、図5に示すセキュリティ情報260に含まれる情報であってもよい。

[0176] 制御ユニット100は、セキュリティユニット200のステータスに基づいて、制御モードを設定する。したがって、制御モードは電源切断前のモードに設定される。コントローラシステム1への電源再投入によるリセットが実行されても、インシデントが解除されるまでは、制御ユニット100の制御モードをS a f eモードに維持することができる。

[0177] 図17は、本実施の形態における制御システムの再稼働処理のフローを説明するための第1の図である。図17には、インシデント解除前の制御システムの処理フローが示されている。

[0178] 図17に示すように、インシデントの検知により、制御ユニット100の制御モードはS a f eモードに移行されている。正常稼働のために、R u nモード変更リクエストが制御ユニット100に入力される（ステップS11

）。制御ランタイム部11は、セキュリティユニット200に対して、インシデントの確認を行う（ステップS12）。セキュリティユニット200の制御ランタイム部21は、セキュリティエンジン250からインシデント情報を取得する（ステップS13）。このインシデント情報は、Runモードへの変更が不可である（「NG」）という情報でもよく、セキュリティレベルを示す情報（セキュリティレベルが「Yellow」）という情報でもよい。制御ランタイム部21は、取得したインシデント情報を、制御ユニット100に送信する（ステップS14）。インシデント情報は、図5に示すセキュリティ情報260に含まれる情報であってもよい。

[0179] 制御ユニット100の制御ランタイム部11は、インシデント情報を制御ランタイム部21から取得する。制御ランタイム部11は、そのインシデント情報に基づき、Runモード変更リクエストに対する応答を出力する（ステップS15）。この応答は、Runモードへの変更が不可である（「NG」）という情報、あるいは、エラーの情報を含むことができる。

[0180] 図18は、本実施の形態における制御システムの再稼働処理のフローを説明するための第2の図である。図18には、インシデント解除後の制御システムの処理フローが示されている。

[0181] まず、インシデントが解除されたことを示す情報がセキュリティユニット200に入力される（ステップS20）。このときの制御ユニット100の制御モードはSafeモードである。

[0182] Runモード変更リクエストが制御ユニット100に入力される（ステップS21）。制御ランタイム部11は、セキュリティユニット200に対して、インシデントの確認を行う（ステップS22）。セキュリティユニット200の制御ランタイム部21は、セキュリティエンジン250からインシデント情報を取得する（ステップS23）。このインシデント情報は、Runモードへの変更が可能である（「OK」）という情報でもよく、セキュリティレベルを示す情報（セキュリティレベルが「Green」）という情報でもよい。制御ランタイム部21は、取得したインシデント情報を、制御ユ

ニット100に送信する（ステップS24）。

[0183] 制御ユニット100の制御ランタイム部11は、インシデント情報を制御ランタイム部21から取得する。制御ランタイム部11は、そのインシデント情報に基づき、制御モードをSafeモードからRunモードに変更する（ステップS25）。さらに、制御ランタイム部11は、変更リクエストに対する応答を出力する（ステップS26）。この応答は、Runモードへの変更が可能である（「OK」）という情報を含むことができる。

[0184] このように、制御ユニット100は、制御ユニットの再起動処理の際に、セキュリティユニット200からのインシデント情報に基づいて、制御モードを決定する。セキュリティに関するインシデントが解除されていない場合には、制御ユニット100を再起動した後も制御モードは縮退モードに設定される。インシデントが解除されていないにもかかわらず、制御ユニットの再起動処理によって制御モードが正常モードに設定されることを防止できる。

[0185] 図18に示したフローでは、制御ユニット100は、インシデントが解除されたことを意味するインシデント情報に基づいて、制御モードをRunモードに変更する。しかし管理者権限を持つユーザ（セキュリティ管理者等）からの命令を上記のインシデント情報に優先させてもよい。たとえばセキュリティレベルがYellowであってもアドミニストレータが復帰可能と判断した場合、制御ユニット100は、アドミニストレータからの入力を受け付けることにより、制御モードをRunモードに復帰させてもよい。たとえば、セキュリティユニット200の誤動作（誤った検知等）によりセキュリティレベルを変更した場合に、制御ユニット100の制御モードを縮退モードから制御モードに戻すことができる。また、インシデントが解除されたことが明らかな場合に、コントローラシステム1を早期に復旧させることができる。

[0186] 以上のように、本実施の形態によれば、制御ユニットを縮退モードから正常モードへと切り替える際に、インシデントが解除されているかどうかを判

断する。インシデントが解除されていない場合、制御モードを縮退モードから正常モードへと遷移することはできない。これにより制御システムの誤った再稼働（インシデントが解除されないまま、制御ユニットを通常時と同様に稼働させること）を防止できるので、セキュリティ被害（２次被害）の拡大を防ぐことができる。したがって、制御装置および制御システムのネットワーク化あるいはインテリジェント化に伴って生じ得る脅威に対する保護の確実性を高めることができる。

[0187] < K. 付記 >

以上説明したように、本実施形態は以下に列挙する開示を含む。

[0188] １．コントローラシステム（１）であって、

制御対象を制御するための制御動作を実行する制御ユニット（１００）と、

前記制御ユニット（１００）に接続され、前記コントローラシステム（１）に対するセキュリティ機能を担当するセキュリティユニット（２００）とを備え、

前記制御ユニット（１００）は、前記制御動作に関する制御モードとして、正常モードと、前記コントローラシステム（１）の限定的な動作を実行するための縮退モードとを有し、前記正常モードと前記縮退モードとは相互に遷移可能であり、

前記セキュリティユニット（２００）は、

前記コントローラシステム（１）における、セキュリティに関するインシデントの有無を検知する検知手段（２５０）を含み、

前記制御ユニット（１００）は、前記検知手段（２５０）により前記インシデントが検知された場合には、前記制御モードを前記縮退モードに遷移させて、前記インシデントの解除が前記検知手段（２５０）によって検知されるまで前記制御モードを前記縮退モードに保つ、コントローラシステム（１）。

[0189] ２．前記制御ユニット（１００）は、前記検知手段（２５０）から前記イ

ンシデントの検知に関するインシデント情報を取得し、

前記インシデント情報が前記インシデントの解除を示す場合には、前記制御ユニット（１００）は、前記縮退モードから前記正常モードへ前記制御モードを変更し、

前記インシデント情報が前記インシデントの継続を示す場合には、前記制御ユニット（１００）は、前記制御モードを前記縮退モードに設定する、１．に記載のコントローラシステム（１）。

[0190] ３．前記制御ユニット（１００）は、前記制御ユニット（１００）の再起動処理を実行する場合に、前記インシデント情報に基づいて、前記制御モードを決定する、２．に記載のコントローラシステム（１）。

[0191] ４．前記セキュリティユニット（２００）は、前記インシデントの検知に関する情報を不揮発的に記憶して、

前記コントローラシステム（１）への電源再投入による前記コントローラシステム（１）の再起動時に、前記セキュリティユニット（２００）は、前記セキュリティユニット（２００）に記憶された前記情報に基づいて、前記セキュリティユニット（２００）のステータスを復帰させ、

前記制御ユニット（１００）は、前記セキュリティユニット（２００）の前記ステータスに基づいて、前記制御モードを設定する、１．から３．のいずれかに記載のコントローラシステム（１）。

[0192] ５．前記セキュリティユニット（２００）は、管理者権限を持つユーザからの操作を前記インシデント情報に優先させて、前記インシデントの検知に関する前記セキュリティユニット（２００）のステータスを変更する、１．から４．のいずれかに記載のコントローラシステム（１）。

[0193] ６．前記縮退モードにおいて、前記制御ユニット（１００）は、前記制御動作を制限する、１．から５．のいずれか１項に記載のコントローラシステム（１）。

[0194] ７．前記縮退モードにおいて、前記制御ユニット（１００）は、前記制御対象の動作を制限する、１．から５．のいずれかに記載のコントローラシ

テム（１）。

[0195] 今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した説明ではなく、請求の範囲によって示され、請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

符号の説明

[0196] １ コントローラシステム、２ 第１ネットワーク、４ 第２ネットワーク、１０ 制御システム、１１，２１ 制御ランタイム部、１００ 制御ユニット、１０２，２０２，３０２ プロセッサ、１０４，２０４，３０４ チップセット、１０６，２０６，３０６ 主記憶装置、１０８，２０８，３０８ 二次記憶装置、１１０，２１０ 通信コントローラ、１１２，２１２ USBコントローラ、１１４，２１４，３１４ メモリカードインターフェイス、１１５，２１５，３１５ メモリカード、１１６，１１８，１２０，２１６，２１８ ネットワークコントローラ、１２２，３２２ 内部バスコントローラ、１２４，２２４，３２４，８２４ インジケータ、１４２，１４４，２４２ 通信ポート、１５０ 制御エンジン、１６０ 情報エンジン、１７０ ブローカー、１８０，３６０ ログデータベース、２００ セキュリティユニット、２５０ セキュリティエンジン、２６０ セキュリティ情報、３００ セーフティユニット、３５０ セーフティエンジン、４００ 機能ユニット、４５０ 電源ユニット、５００ フィールドデバイス、６００ サポート装置、７００ SCADA装置、８００ HMI、９００ データベース、Ｓ１～Ｓ１０６ ステップ。

請求の範囲

[請求項1]

コントローラシステムであって、
制御対象を制御するための制御動作を実行する制御ユニットと、
前記制御ユニットに接続され、前記コントローラシステムに対するセキュリティ機能を担当するセキュリティユニットとを備え、
前記制御ユニットは、前記制御動作に関する制御モードとして、正常モードと、前記コントローラシステムの限定的な動作を実行するための縮退モードとを有し、前記正常モードと前記縮退モードとは相互に遷移可能であり、
前記セキュリティユニットは、
前記コントローラシステムにおける、セキュリティに関するインシデントの有無を検知する検知手段を含み、
前記制御ユニットは、前記検知手段により前記インシデントが検知された場合には、前記制御モードを前記縮退モードに遷移させて、前記インシデントの解除が前記検知手段によって検知されるまで前記制御モードを前記縮退モードに保つ、コントローラシステム。

[請求項2]

前記制御ユニットは、前記検知手段から前記インシデントの検知に関するインシデント情報を取得し、
前記インシデント情報が前記インシデントの解除を示す場合には、前記制御ユニットは、前記縮退モードから前記正常モードへ前記制御モードを変更し、
前記インシデント情報が前記インシデントの継続を示す場合には、前記制御ユニットは、前記制御モードを前記縮退モードに設定する、請求項1に記載のコントローラシステム。

[請求項3]

前記制御ユニットは、前記制御ユニットの再起動処理を実行する場合に、前記インシデント情報に基づいて、前記制御モードを決定する、請求項2に記載のコントローラシステム。

[請求項4]

前記セキュリティユニットは、前記インシデントの検知に関する情

報を不揮発的に記憶して、

前記コントローラシステムへの電源再投入による前記コントローラシステムの再起動時に、前記セキュリティユニットは、前記セキュリティユニットに記憶された前記情報に基づいて、前記セキュリティユニットのステータスを復帰させ、

前記制御ユニットは、前記セキュリティユニットの前記ステータスに基づいて、前記制御モードを設定する、請求項1から請求項3のいずれか1項に記載のコントローラシステム。

[請求項5] 前記セキュリティユニットは、管理者権限を持つユーザからの操作を前記インシデント情報に優先させて、前記インシデントの検知に関する前記セキュリティユニットのステータスを変更する、請求項1から請求項4のいずれか1項に記載のコントローラシステム。

[請求項6] 前記縮退モードにおいて、前記制御ユニットは、前記制御動作を制限する、請求項1から請求項5のいずれか1項に記載のコントローラシステム。

[請求項7] 前記縮退モードにおいて、前記制御ユニットは、前記制御対象の動作を制限する、請求項1から請求項5のいずれか1項に記載のコントローラシステム。

[図1]

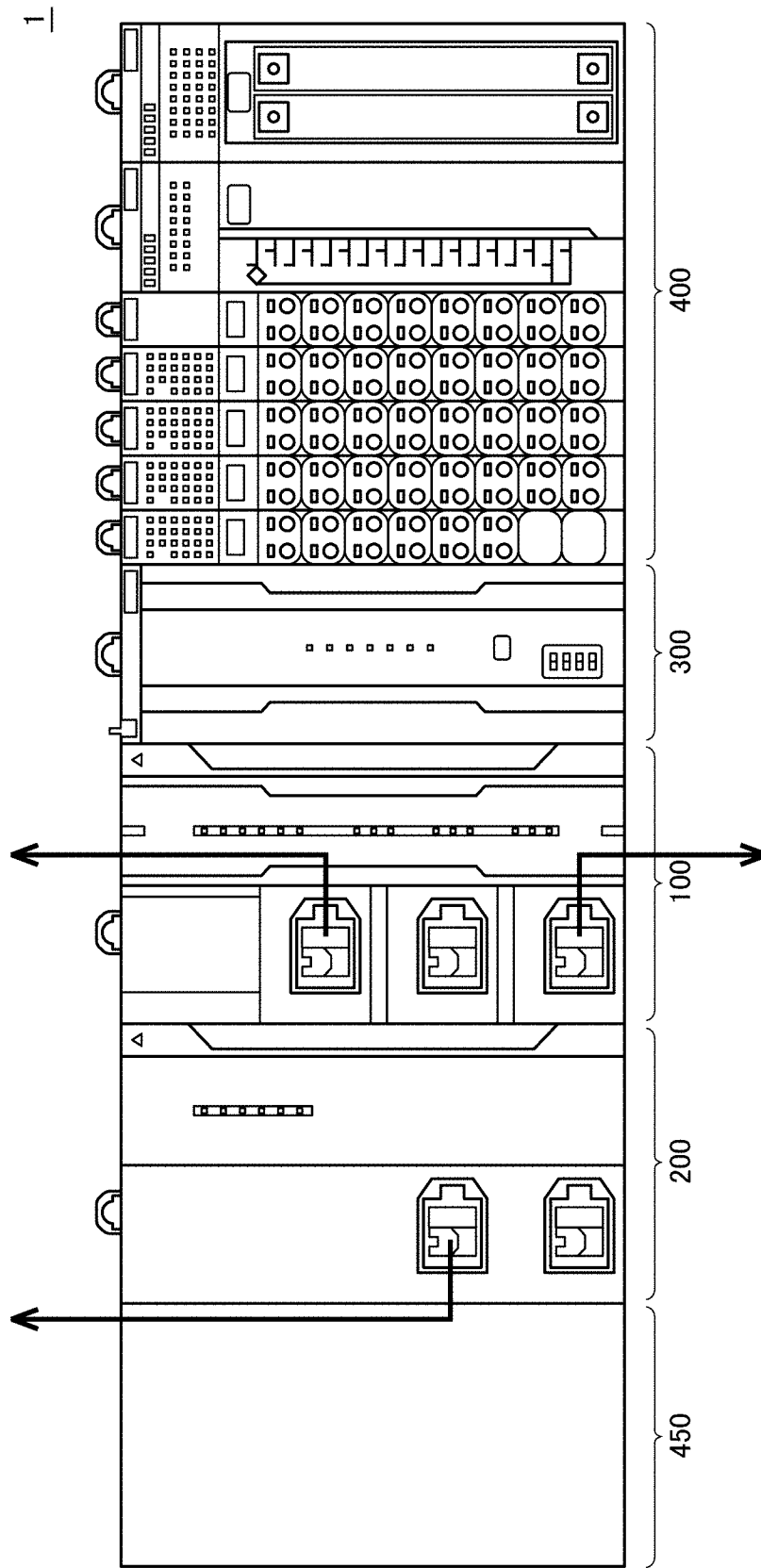
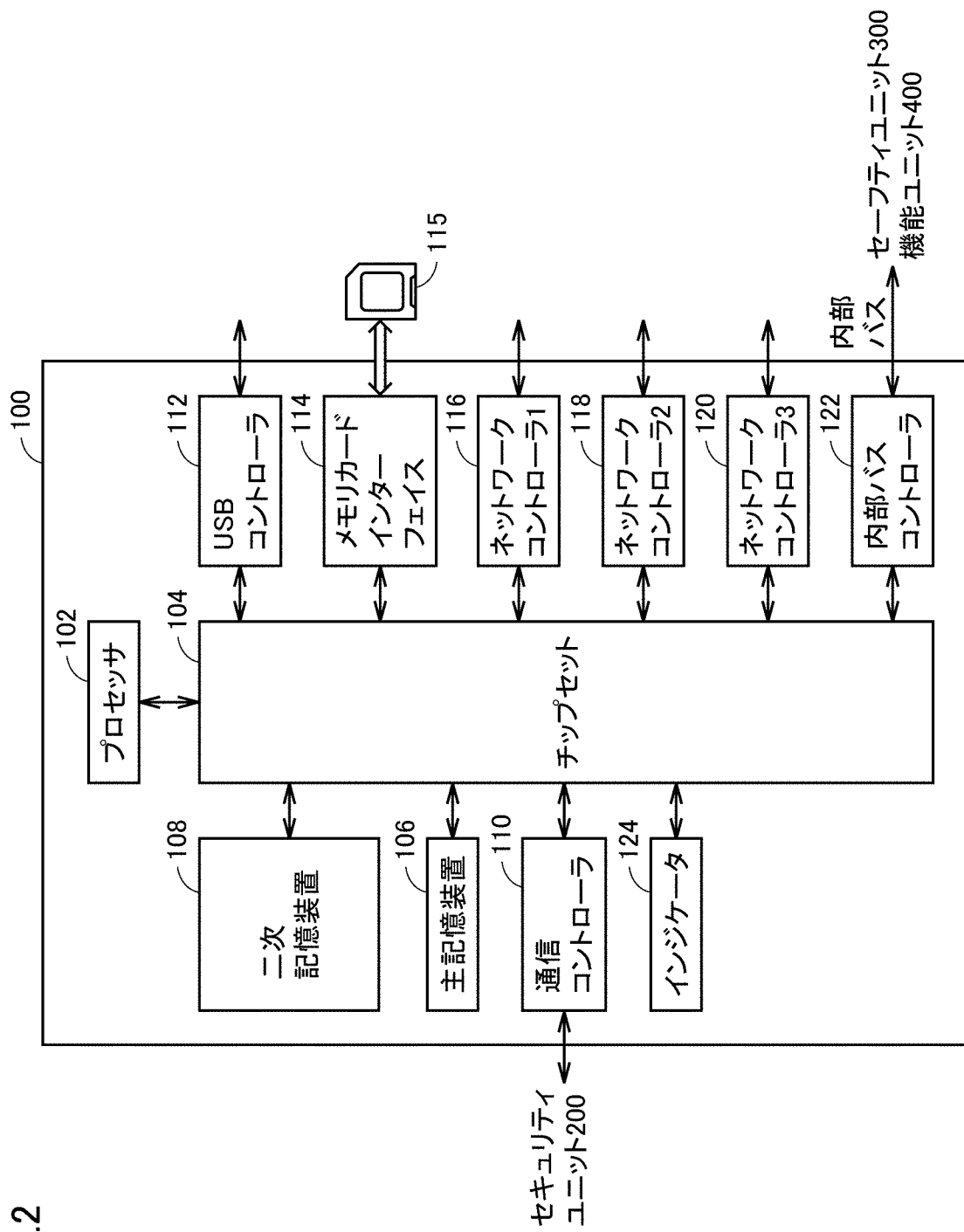


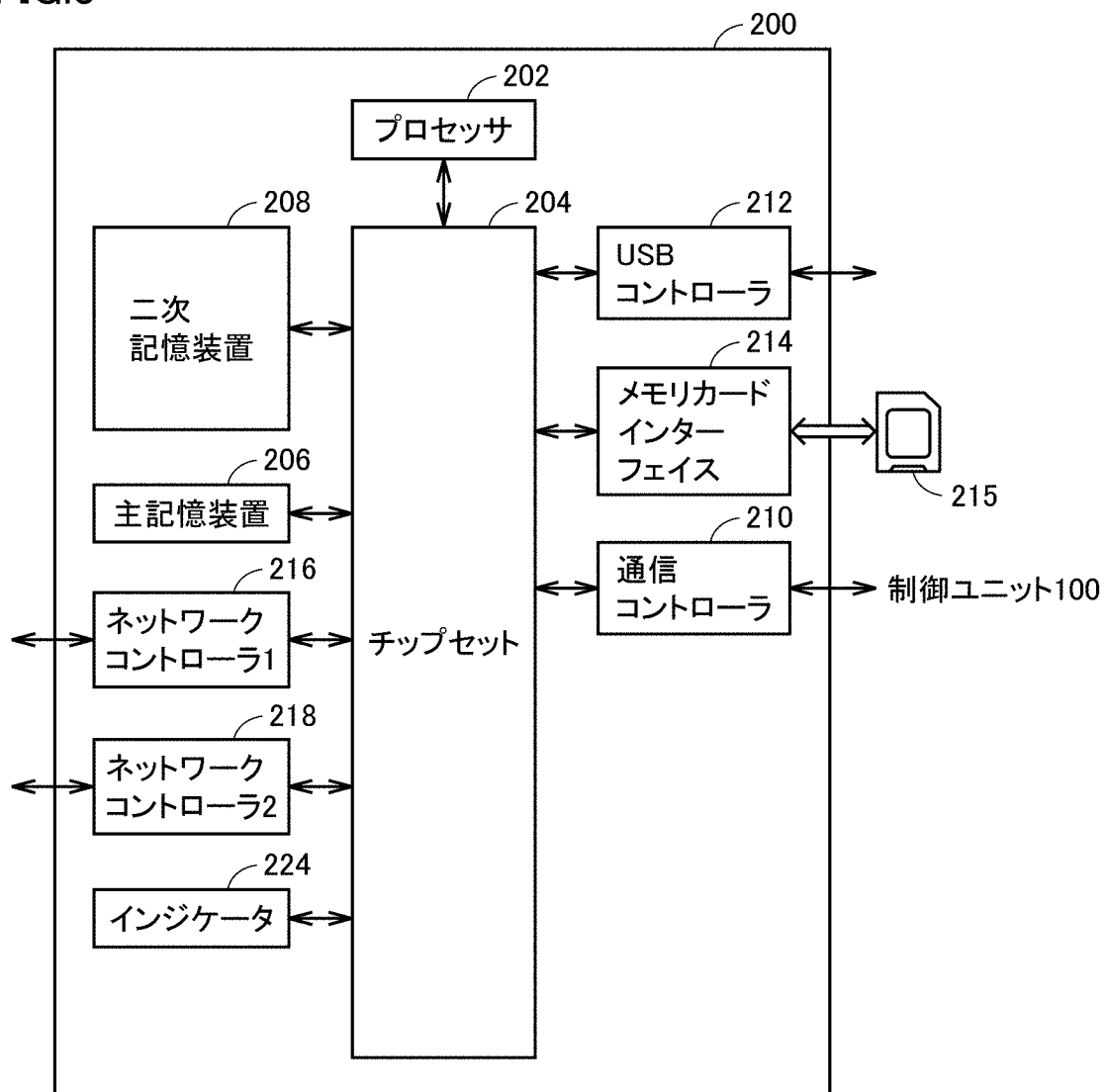
FIG.1

[図2]



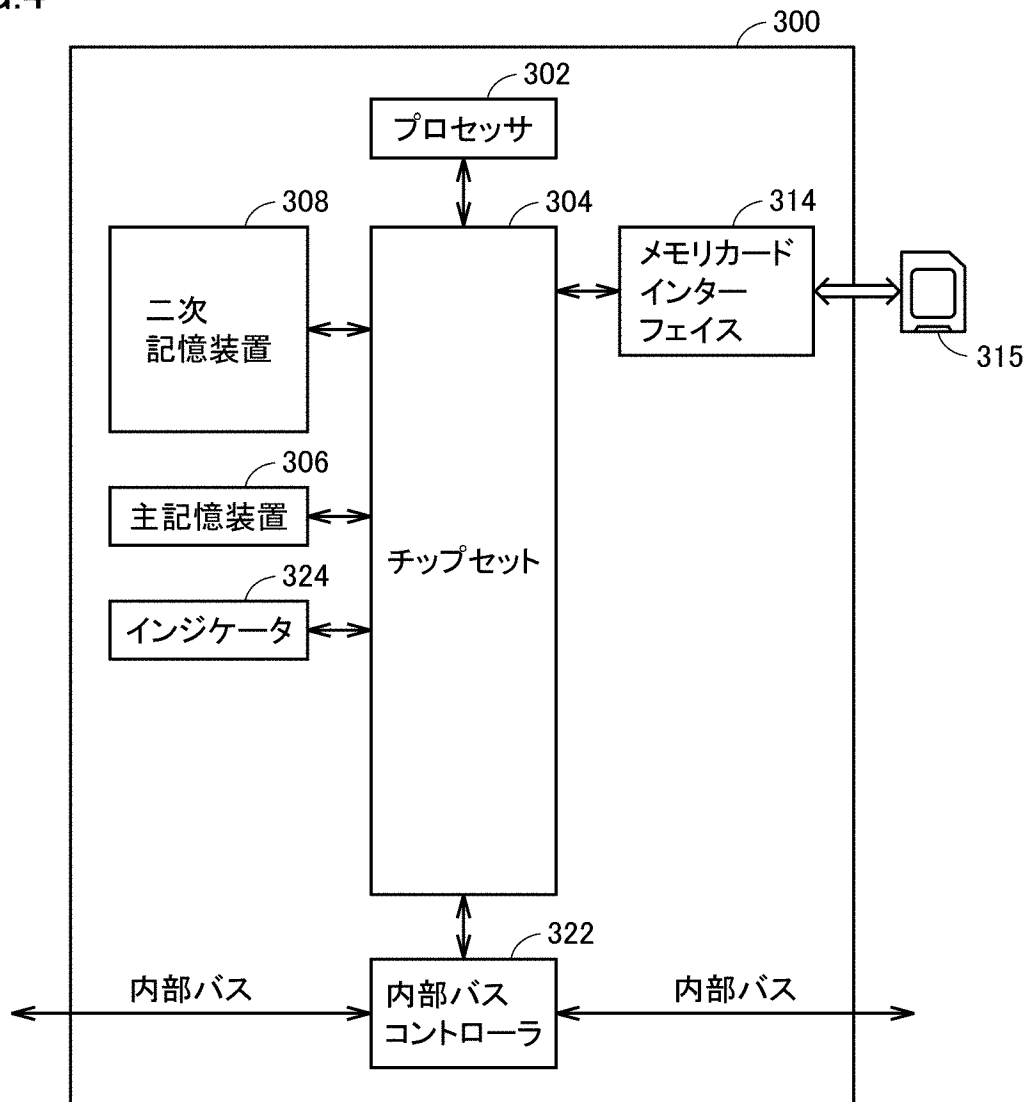
[図3]

FIG.3



[図4]

FIG.4



[図6]

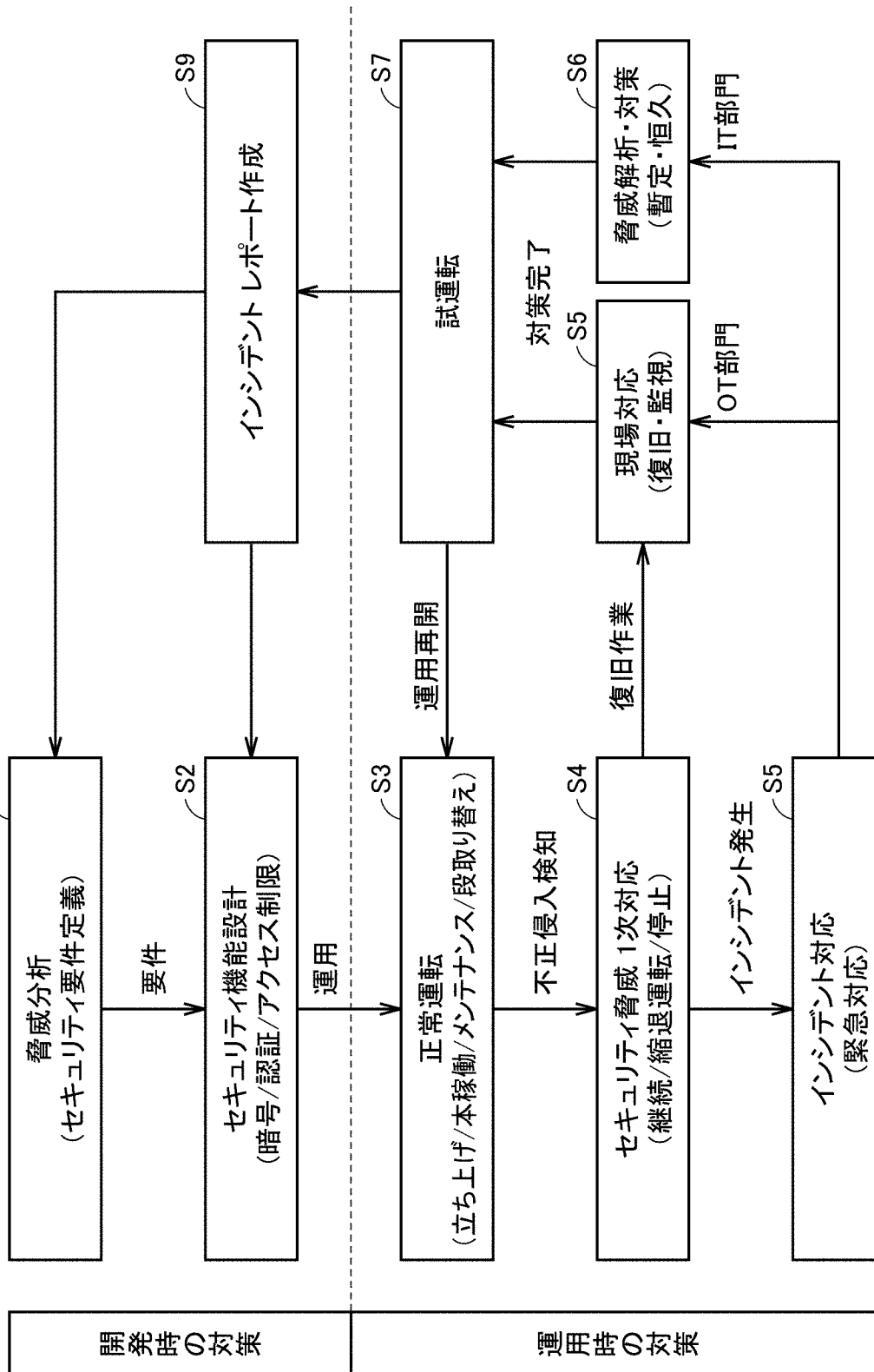


FIG. 6

[図8]

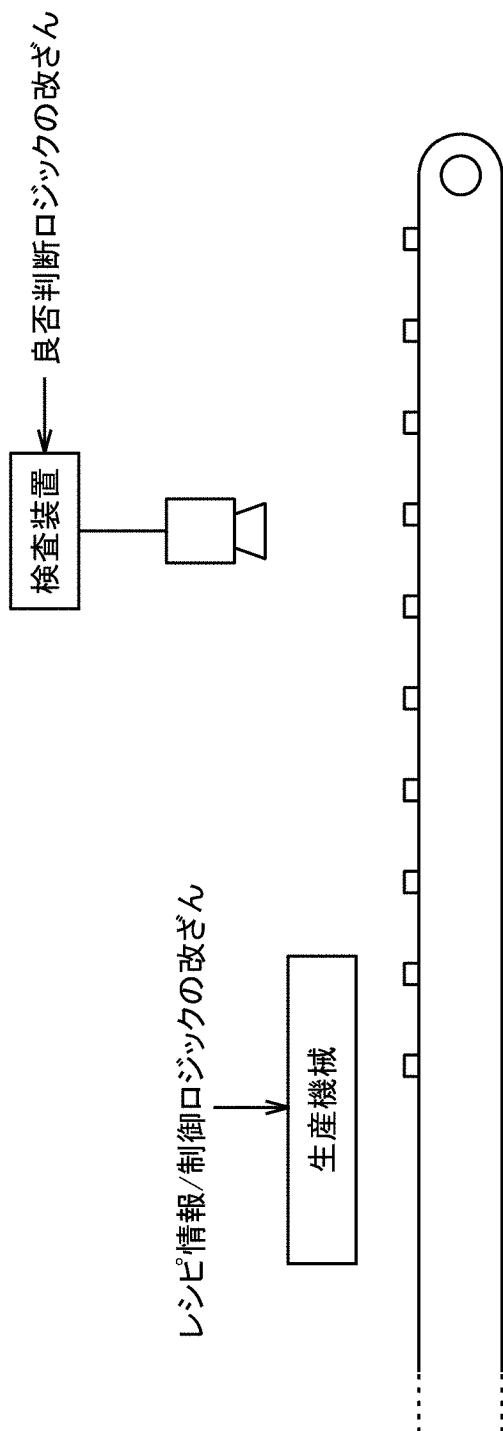


FIG.8

[図9]

FIG.9

インシデント特性	設備A	設備B	設備C
無し(正常運転)	設備制御: 正常運転 情報通信: 正常運転	設備制御: 正常運転 情報通信: 正常運転	設備制御: 正常運転 情報通信: 正常運転
無作為改ざん	設備制御: 正常運転 情報通信: 縮退A1	設備制御: 正常運転 情報通信: 正常運転	設備制御: 縮退C1 情報通信: 縮退C2
リソース枯渇	設備制御: 縮退A2 情報通信: 縮退A3	設備制御: 縮退B1 情報通信: 縮退B2	設備制御: 停止 情報通信: 縮退C3
DDoS攻撃	設備制御: 停止 情報通信: 縮退A4	設備制御: 正常運転 情報通信: 縮退B3	設備制御: 停止 情報通信: 縮退C4
...			

[図10]

FIG.10

インシデント特性	設備A	設備B	設備C
無し(正常運転)	設備制御: 正常運転 情報通信: 正常運転	設備制御: 正常運転 情報通信: 正常運転	設備制御: 正常運転 情報通信: 正常運転
レベル1	設備制御: 正常運転 情報通信: 縮退A1	設備制御: 正常運転 情報通信: 正常運転	設備制御: 正常運転 情報通信: 縮退C1
レベル2	設備制御: 縮退A2 情報通信: 縮退A3	設備制御: 縮退B1 情報通信: 縮退B2	設備制御: 正常運転 情報通信: 縮退C2
レベル3	設備制御: 停止 情報通信: 縮退A4	設備制御: 停止 情報通信: 縮退B3	設備制御: 縮退C3 情報通信: 縮退C4

[図11]

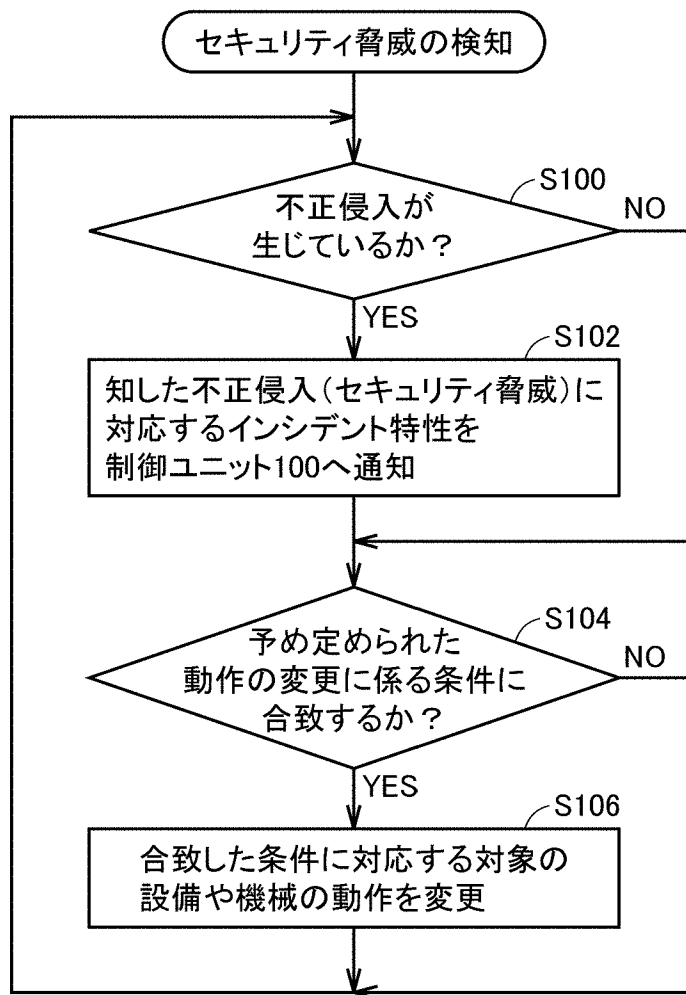
FIG.11

.....

インシデント特性		設備C		設備C	
インシデント特性		設備B		設備B	
インシデント特性		設備A (運転)	設備A (メンテナンス)	設備A (段取り替え)	
無し(正常運転)		設備制御: 正常運転 情報通信: 正常運転	設備制御: 正常運転 情報通信: 正常運転	設備制御: 正常運転 情報通信: 正常運転	
無作為改ざん		設備制御: 正常運転 情報通信: 縮退A1	設備制御: 正常運転 情報通信: 正常運転	設備制御: 正常運転 情報通信: 縮退A1	
リソース枯渇		設備制御: 縮退A2 情報通信: 縮退A3	設備制御: 正常運転 情報通信: 縮退A7	設備制御: 縮退A2 情報通信: 縮退A3	
DDoS攻撃		設備制御: 縮退A4 情報通信: 縮退A5	設備制御: 縮退A8 情報通信: 縮退A9	設備制御: 縮退A4 情報通信: 縮退A10	
...					

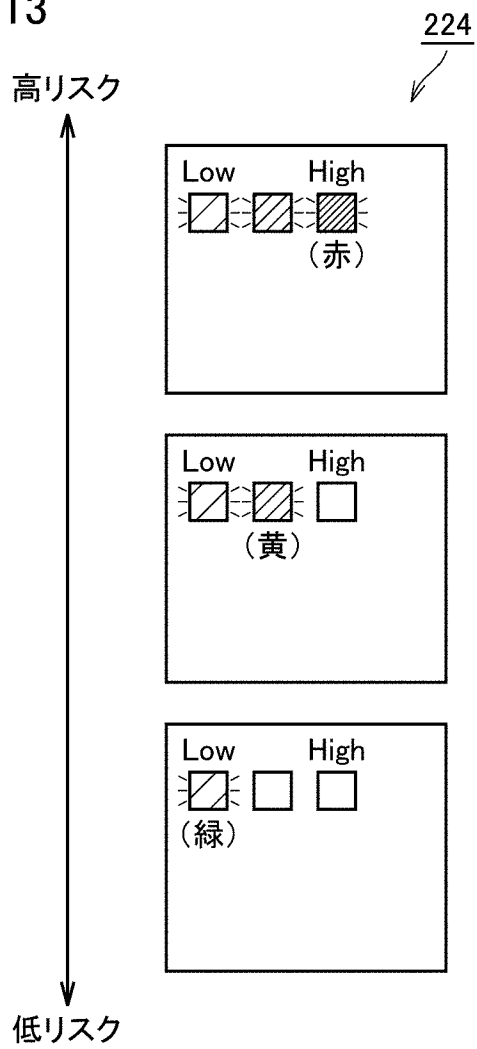
[図12]

FIG.12



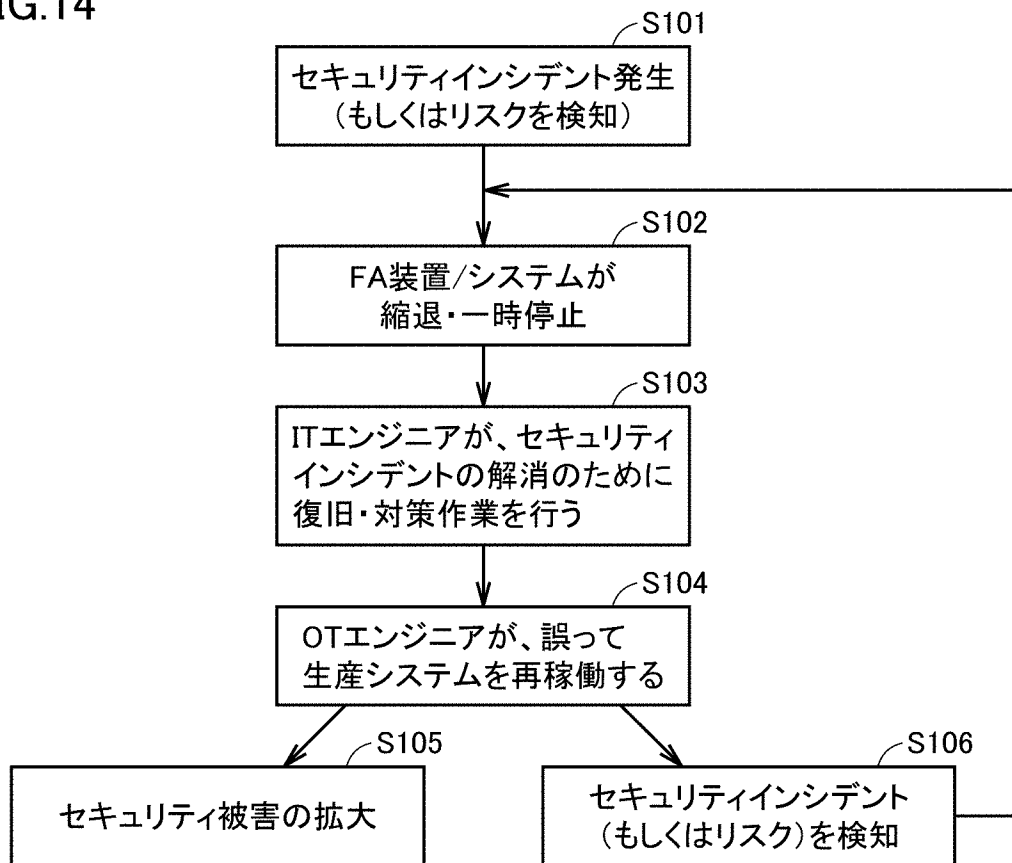
[図13]

FIG.13

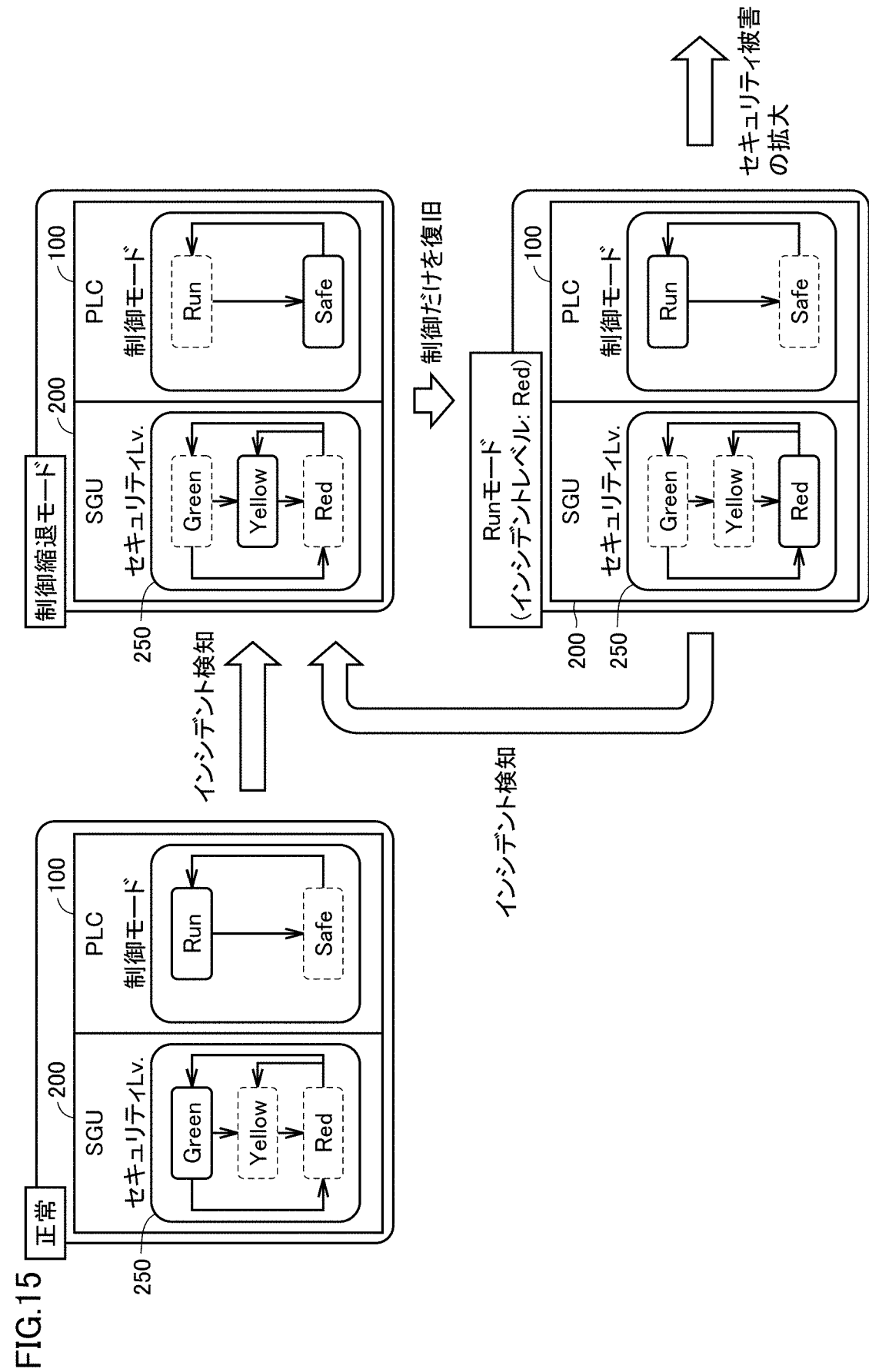


[図14]

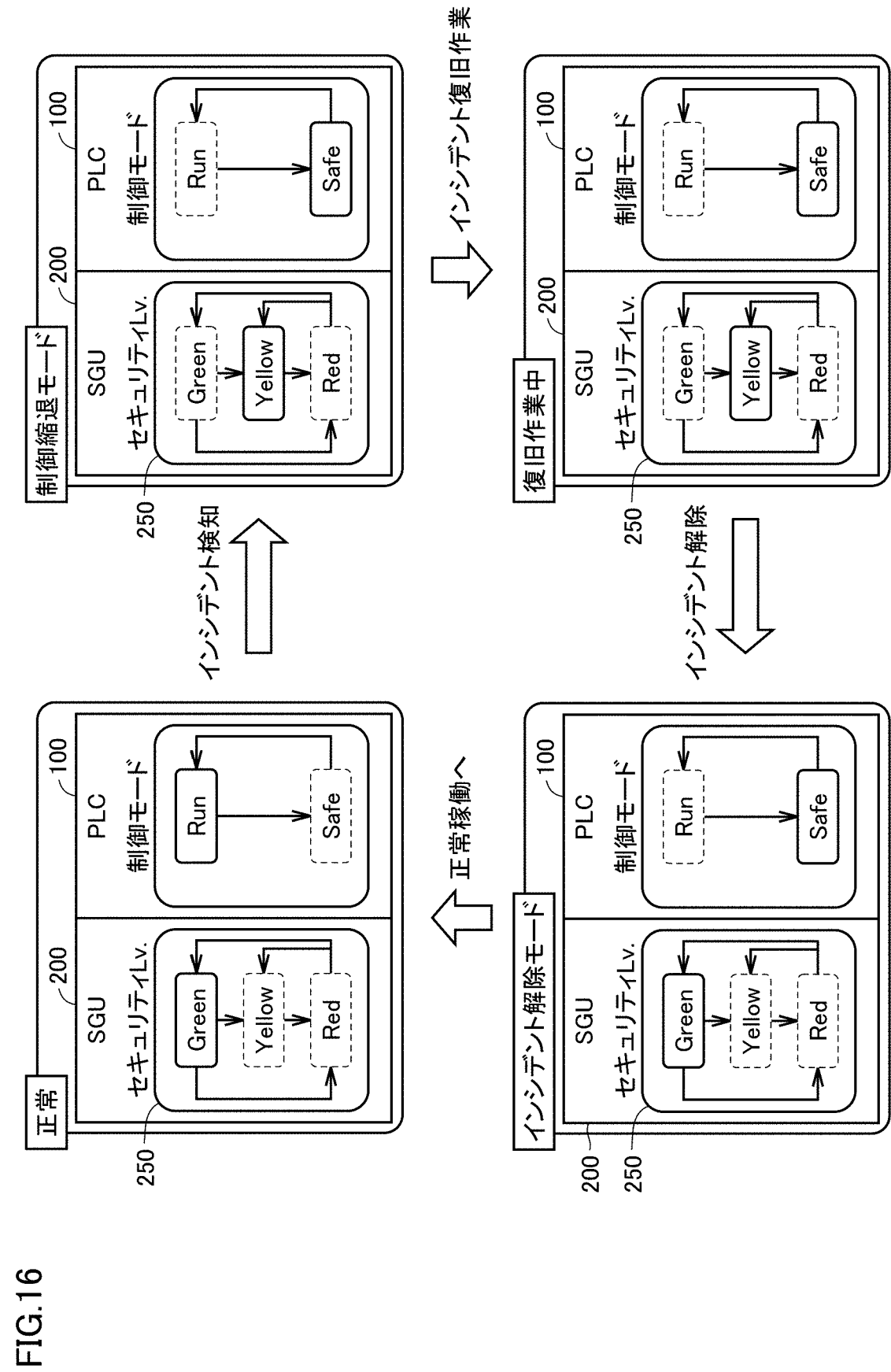
FIG.14



[図15]

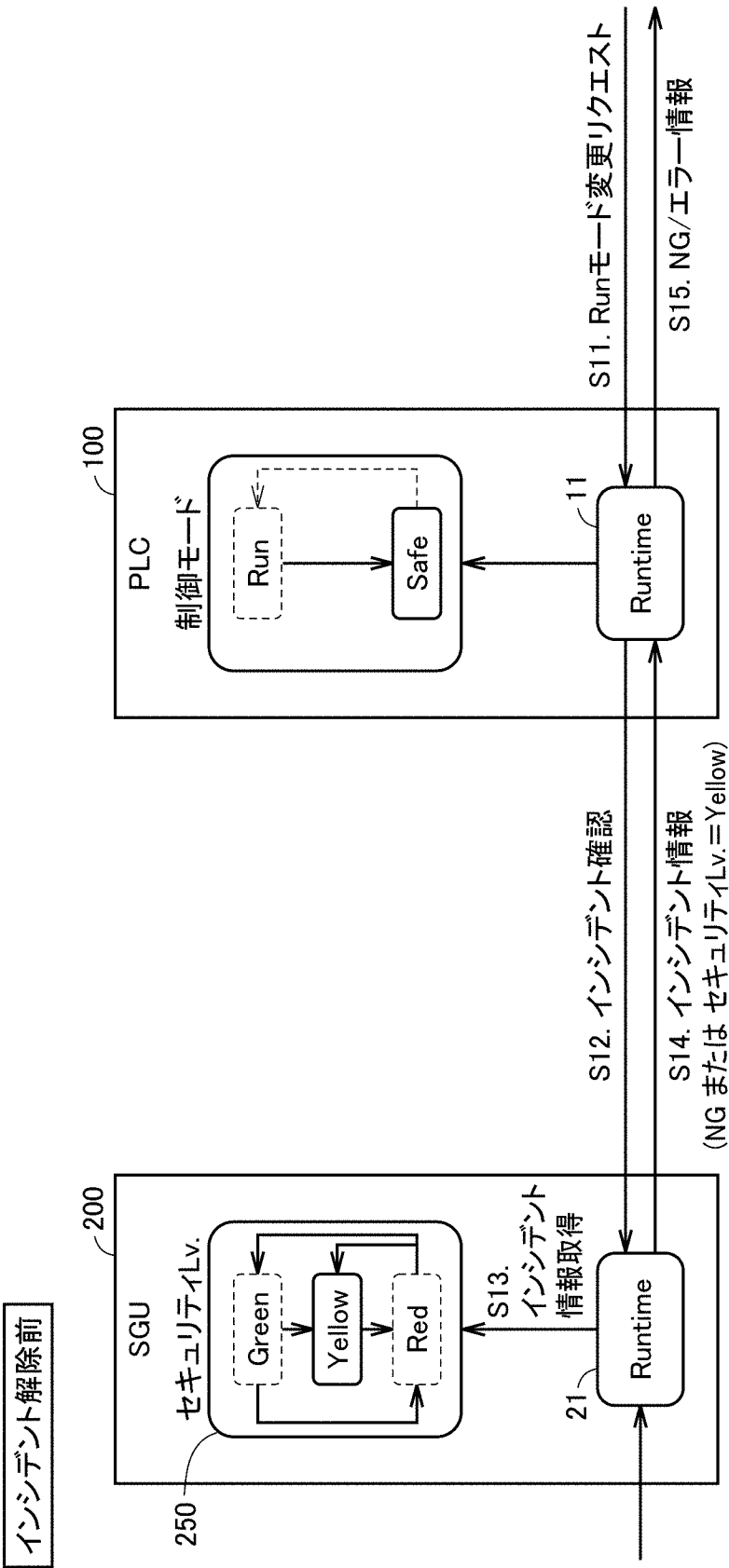


[図16]



[図17]

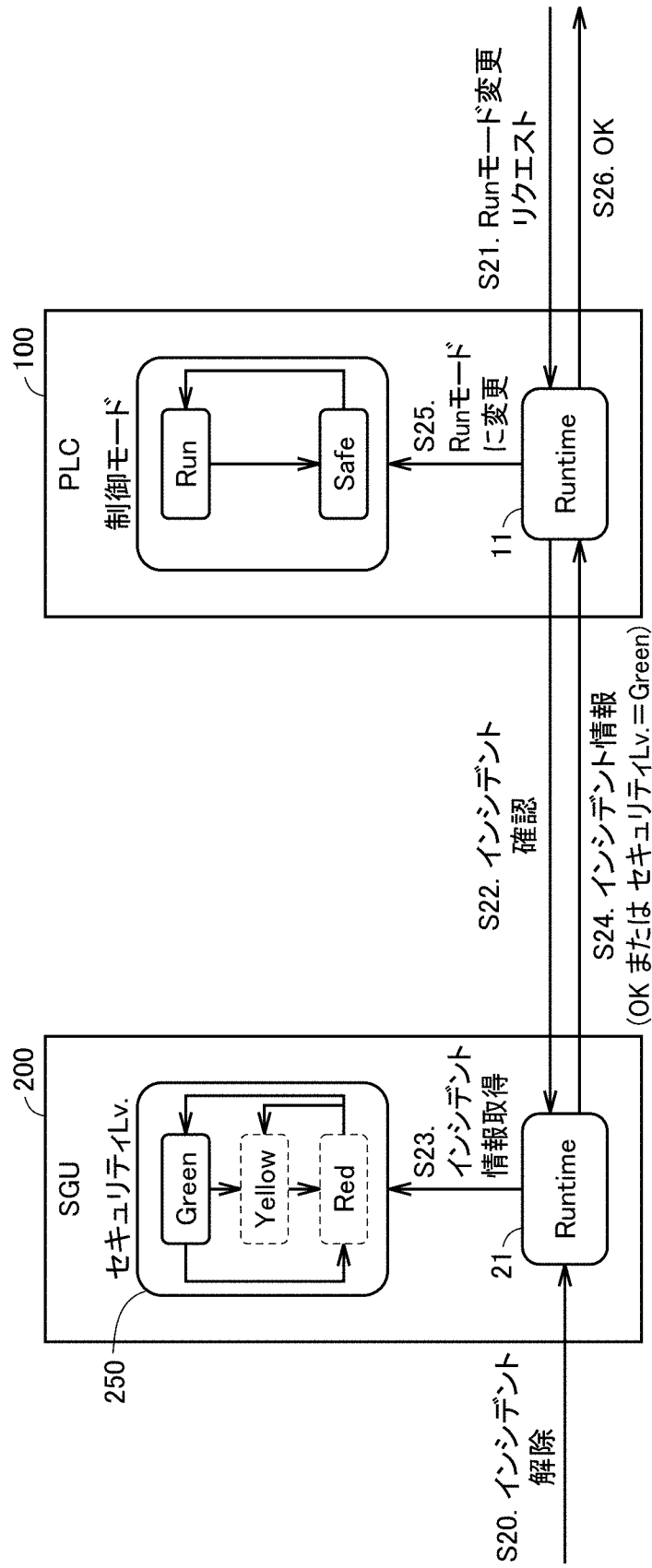
FIG.17



[図18]

FIG.18

インシデント解除後



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2020/007802

A. CLASSIFICATION OF SUBJECT MATTER

G05B 19/05 (2006.01) i; G05B 9/02 (2006.01) i
FI: G05B19/05 Z; G05B9/02 C

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G05B19/05; G05B9/02

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Published examined utility model applications of Japan	1922-1996
Published unexamined utility model applications of Japan	1971-2020
Registered utility model specifications of Japan	1996-2020
Published registered utility model applications of Japan	1994-2020

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 2015/001594 A1 (HITACHI, LTD.) 08.01.2015 (2015-01-08) paragraphs [0012]-[0033], fig. 2-5	1-7
Y	JP 2018-200731 A (OMRON CORP.) 20.12.2018 (2018-12-20) paragraphs [0081]-[0087], [0111]-[0126], fig. 7-8, 13-14	1-7
Y	JP 60-159904 A (HITACHI, LTD.) 21.08.1985 (1985-08-21) page 2, lower left column, lines 4-14	3-4

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"I" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

07 April 2020 (07.04.2020)

Date of mailing of the international search report

21 April 2020 (21.04.2020)

Name and mailing address of the ISA/

Japan Patent Office
3-4-3, Kasumigaseki, Chiyoda-ku,
Tokyo 100-8915, Japan

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/JP2020/007802

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
WO 2015/001594 A1	08 Jan. 2015	US 2015/0295944 A1	
		paragraphs [0024]-	
		[0045], fig. 2-5	
JP 2018-200731 A	20 Dec. 2018	(Family: none)	
JP 60-159904 A	21 Aug. 1985	(Family: none)	

A. 発明の属する分野の分類（国際特許分類（IPC）） G05B 19/05(2006.01)i; G05B 9/02(2006.01)i FI: G05B19/05 Z; G05B9/02 C														
B. 調査を行った分野 調査を行った最小限資料（国際特許分類（IPC）） G05B19/05; G05B9/02 最小限資料以外の資料で調査を行った分野に含まれるもの <table border="0"> <tr> <td>日本国実用新案公報</td> <td>1922 - 1996年</td> </tr> <tr> <td>日本国公開実用新案公報</td> <td>1971 - 2020年</td> </tr> <tr> <td>日本国実用新案登録公報</td> <td>1996 - 2020年</td> </tr> <tr> <td>日本国登録実用新案公報</td> <td>1994 - 2020年</td> </tr> </table> 国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）			日本国実用新案公報	1922 - 1996年	日本国公開実用新案公報	1971 - 2020年	日本国実用新案登録公報	1996 - 2020年	日本国登録実用新案公報	1994 - 2020年				
日本国実用新案公報	1922 - 1996年													
日本国公開実用新案公報	1971 - 2020年													
日本国実用新案登録公報	1996 - 2020年													
日本国登録実用新案公報	1994 - 2020年													
C. 関連すると認められる文献														
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号												
Y	WO 2015/001594 A1（株式会社日立製作所）08.01.2015（2015 - 01 - 08） 段落[0012]-[0033], 図2-5	1-7												
Y	JP 2018-200731 A（オムロン株式会社）20.12.2018（2018 - 12 - 20） 段落[0081]-[0087], [0111]-[0126], 図7-8, 13-14	1-7												
Y	JP 60-159904 A（株式会社日立製作所）21.08.1985（1985 - 08 - 21） 第2ページ左下欄第4行-第14行	3-4												
☐ C欄の続きにも文献が列挙されている。 ☒ パテントファミリーに関する別紙を参照。														
<table border="0"> <tr> <td>* 引用文献のカテゴリー</td> <td>“T” 国際出願日又は優先日後に公表された文献であって出願と抵触するものではなく、発明の原理又は理論の理解のために引用するもの</td> </tr> <tr> <td>“A” 特に関連のある文献ではなく、一般的技術水準を示すもの</td> <td>“X” 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの</td> </tr> <tr> <td>“E” 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの</td> <td>“Y” 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの</td> </tr> <tr> <td>“L” 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）</td> <td>“&” 同一パテントファミリー文献</td> </tr> <tr> <td>“O” 口頭による開示、使用、展示等に言及する文献</td> <td></td> </tr> <tr> <td>“P” 国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献</td> <td></td> </tr> </table>			* 引用文献のカテゴリー	“T” 国際出願日又は優先日後に公表された文献であって出願と抵触するものではなく、発明の原理又は理論の理解のために引用するもの	“A” 特に関連のある文献ではなく、一般的技術水準を示すもの	“X” 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの	“E” 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの	“Y” 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの	“L” 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）	“&” 同一パテントファミリー文献	“O” 口頭による開示、使用、展示等に言及する文献		“P” 国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献	
* 引用文献のカテゴリー	“T” 国際出願日又は優先日後に公表された文献であって出願と抵触するものではなく、発明の原理又は理論の理解のために引用するもの													
“A” 特に関連のある文献ではなく、一般的技術水準を示すもの	“X” 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの													
“E” 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの	“Y” 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの													
“L” 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）	“&” 同一パテントファミリー文献													
“O” 口頭による開示、使用、展示等に言及する文献														
“P” 国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献														
国際調査を完了した日 07.04.2020	国際調査報告の発送日 21.04.2020													
名称及びあて先 日本国特許庁(ISA/JP) 〒100-8915 日本国 東京都千代田区霞が関三丁目4番3号	権限のある職員（特許庁審査官） 影山 直洋 3U 5785 電話番号 03-3581-1101 内線 3364													

国際調査報告
パテントファミリーに関する情報

国際出願番号

PCT/JP2020/007802

引用文献			公表日	パテントファミリー文献	公表日
WO	2015/001594	A1	08.01.2015	US 2015/0295944 A1 段落[0024]-[0045], 図2-5	
JP	2018-200731	A	20.12.2018	(ファミリーなし)	
JP	60-159904	A	21.08.1985	(ファミリーなし)	